Version 7.8 | November 2012 | DOC2702A

Polycom® RealPresence® Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide

This software has not achieved UC APL certification.

This document provides the latest information for security-conscious users running Version 7.8 software. The information in this document is not intended to imply that DoD or DISA certifies Polycom RMX systems.

For regulatory notices see individual Polycom® RealPresence® Collaboration Server (RMX®) 1500/2000/4000 Hardware Guides.

Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA

Table of Contents

1

Overview

About the RMX Administrator's Guide

The product names, *Polycom® RealPresence® Collaboration Server 1500, 2000, 4000* and *RMX® 1500, 2000, 4000* are used interchangeably throughout this document.

The *Polycom® Polycom® RealPresence® Collaboration Server 1500, 2000, 4000* provides instructions for configuring, deploying, and administering Polycom Multipoint Control Units (MCUs) for video conferencing. This guide will help you understand the Polycom video conferencing components, and provides descriptions of all available conferencing features. This guide will help you perform the following tasks:

- Customize the RMX conferencing entities such as conference Profiles, IVR Services, Meeting Rooms, Entry Queues, etc., to your organization's needs.
- Define RMX Users.
- Further customize the RMX Network Settings for ISDN networks, IP networks for Ultra Secure Mode, and IPv6 environments.
- Advanced conference Management
- Define Video Protocols and Resolution Configuration for CP Conferencing
- Configure Templates, the Address Book and Schedule Reservations
- Record Conferences
- Configure the RMX to support special call flows and conferencing requirements, such as Cascading Conferences and Gateway Calls.
- Configure the RMX to support Polycom third party and partner environments such as Microsoft, IBM, Cisco, Avaya, Broadsoft and Siemens.
- Configure the RMX for special applications and needs by setting various system flags.
- Manage and troubleshoot the RMX's performance.

The *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide* provides description of basic conferencing operations. It will help you perform the following tasks:

- Unpack the RMX system and install it on a a rack.
- Connect the required cables to the RMX.
- Perform basic configuration procedures.
- Start a new conference and connect participants/endpoints to it.
- Monitor ongoing conferences
- Perform basic operations and monitoring tasks

The *RealPresence Collaboration Server (RMX) 1500/2000/4000 Deployment Guide for Maximum Security Environments* provides a deployment methodology for system administrators implementing *Maximum Security Environments*.

Who Should Read This Guide?

System administrators and network engineers should read this guide to learn how to properly set up Polycom RMX systems. This guide describes administration-level tasks.

For detailed description of first time installation and configuration, description of the RMX *Web Client,* and basic operation of your RMX system, see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide.

Prerequisites

This guide assumes the user has the following knowledge:

- Familiarity with Windows® XP or Vista® operating systems and interface.
- Familiarity with Microsoft® Internet Explorer® Version 7 or higher.
- Basic knowledge of video conferencing concepts and terminology.

How This Guide is Organized

The following typographic conventions are used in this guide to distinguish types of in-text information.

Table 1-1 *Typographic Conventions*

Convention	Description
Bold	Highlights interface items such as menus, soft keys, flag names, and directories. Also used to represent menu selections and text entry to the phone.
Italics	Used to emphasize text, to show example values or inputs, file names and to show titles of reference documents available from the Polycom Support Web site and other reference sites.
Underlined Blue	Used for URL links to external Web pages or documents. If you click on text in this style, you will be linked to an external document or Web page.
Blue Text	Used for cross referenced page numbers in the same or other chapters or documents. If you click on blue text, you will be taken to the referenced section. Also used for cross references. If you click the italic cross reference text, you will be taken to the referenced section.
<variable name>	Indicates a variable for which you must enter information specific to your installation, endpoint, or network. For example, when you see <IP address>, enter the IP address of the described device.
>	Indicates that you need to select an item from a menu. For example, **Administration > System Information** indicates that you need to select **System Information** from the *Administration* menu.

About the Polycom RMX System

The Polycom RMX 1500/2000/4000 Multipoint Control Unit (MCU) is a high performance, scalable, IP-network (H.323 and SIP) and ISDN/PSTN solution that provides the user with feature-rich and easy-to-use multipoint voice and video conferencing.

The RMX 1500/2000/4000 unit can be controlled via the LAN, the *RMX Web Client* application, Internet Explorer® installed on the user's workstation, or the RMX Manager application. The RMX Manager can control several RMX units (RealPresence Collaboration Server (RMX) 1500, RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000). For more information about the RMX Manager, see "*RMX Manager Application"* on page **20-1**.

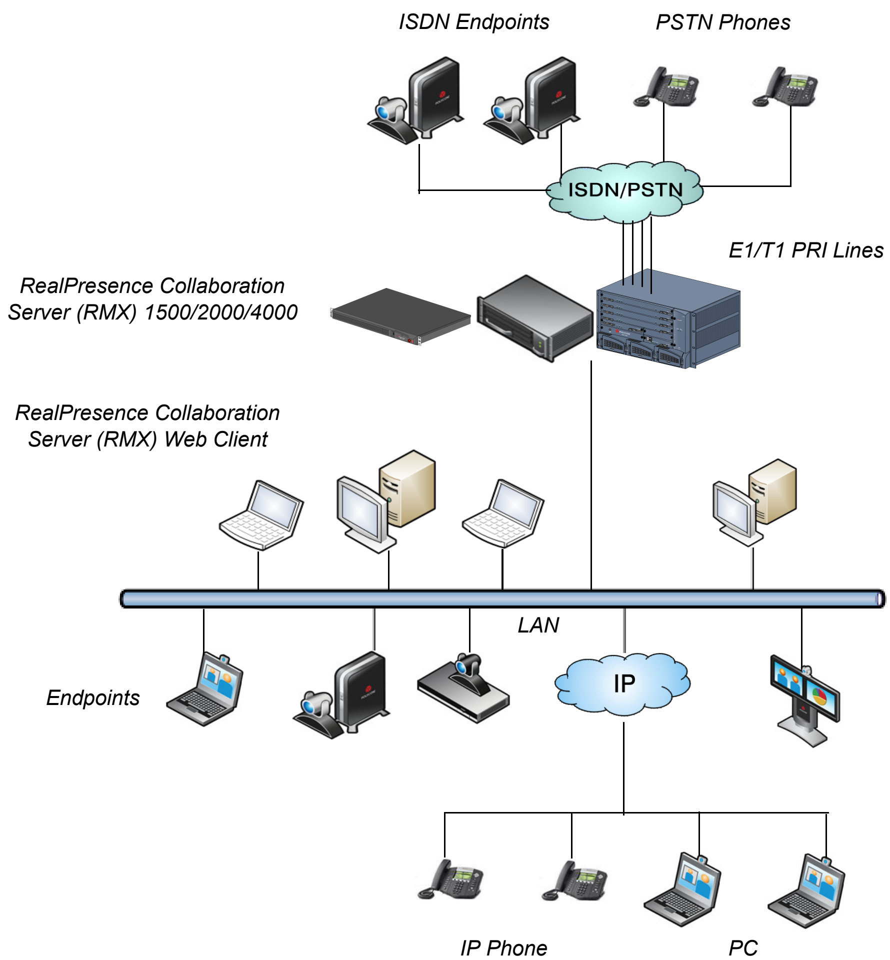


Figure 1-1 *Multipoint Video Conferencing using a RMX 1500/2000/4000*

IP and ISDN Network Guidelines

IP Networks

In the RealPresence Collaboration Server (RMX) 1500 and RealPresence Collaboration Server (RMX) 2000, system management and IP conferencing are performed via a single LAN port. The networks can be separated in Maximum Security Environments.

In the RealPresence Collaboration Server (RMX) 4000, system management and IP conferencing are performed via two different LAN ports. The networks can be separated in Maximum Security Environments.

ISDN Networks

RealPresence Collaboration Server (RMX) 1500 supports one ISDN card with up to 4 E1/T1 PRI lines.

RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000 support a maximum of two RTM ISDN cards, each providing connection for up to either 7 E1 or 9 T1 PRI lines.

On the RMX 1500/2000/4000, E1 and T1 connections cannot be used simultaneously.

For more detailed information about RMX abilities, see the RealPresence Collaboration Server (RMX) Hardware Guides, *Hardware Description, Chapter 1*.

Card Configuration Modes

The media card installed in the system determines the *Card Configuration Mode*. The *Card Configuration Mode* represents different generations of the media card. Each new generation provides additional functionality, higher video resolutions and higher resource capacity.

Only one Media Card **type** can be installed in any RMX, which sets the *Card Configuration Mode* for that RMX:

- **MPM Card Configuration Mode** – Supported with *MPM cards* in all RealPresence Collaboration Server (RMX) 2000 versions prior to Version 7.1.

From *Version 7.1*, *MPM* media cards **are not** supported.

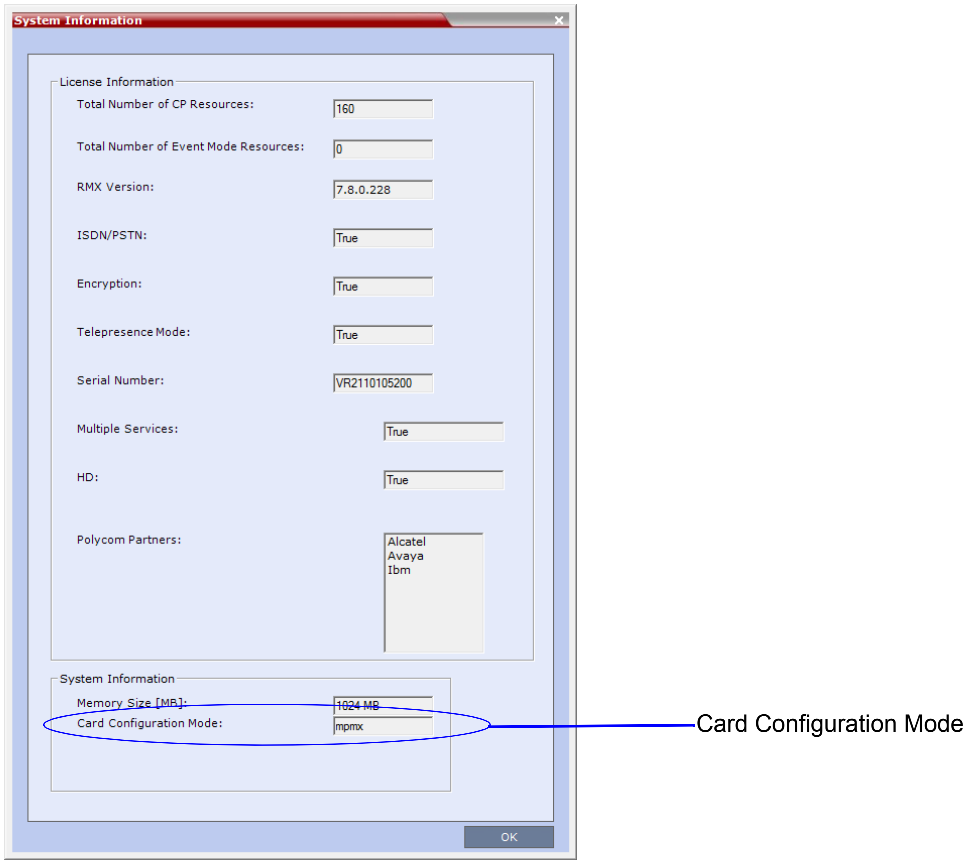
- **MPM+ Card Configuration Mode** – Supported **from Version 4.0**, with *MPM+ cards* installed in the RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000.
- **MPMx Card Configuration Mode** – Supported **from Version 7.0**, with *MPMx cards* installed in the RealPresence Collaboration Server (RMX) 1500, RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000.

Viewing the Card Configuration Mode

The *Card Configuration Mode* is determined according to the installed media card.

The *Licensing Mode* and the *Card Configuration Mode* for your MCU can be viewed in the *System Information* dialog box (go to **Administration > System Information**).

In the example shown here, the RealPresence Collaboration Server *Licensing Mode* is *CP Licensing*, and the *Card Configuration Mode* is *MPMx*.



Feature Support with MPMx Cards Only

Table 1-2 lists the RMX (RMX) features that are only supported with MPMx cards. .

Table 1-2 *Features Supported with MPMx Card Configuration Mode Only*

Feature Name	Description
Scalable Video Coding (SVC)	Scalable Video Coding (SVC) Conferencing, based on the SVC video protocol and SAC audio protocol. SVC Conferencing offers high resolution video conferencing with low end-to-end latency, improved Error Resiliency and higher system capacities.
H.264 High Profile Support	The *H.264 High Profile* improves video quality and can reduce bandwidth requirements for video conferencing transmissions by up to 50%. Supported in IP and ISDN calls.
Support of Symmetric HD Resolutions	Support of symmetric *HD* video resolutions *HD 1080p30* and *HD 720p60*.
w448 Resolution support	Improves interoperability with *Tandberg MXP 990/3000* endpoints providing these endpoints the resolution of *W448p* (768x448 pixels) at 25fps.

Table 1-2 *Features Supported with MPMx Card Configuration Mode Only*

Feature Name	Description
Content at HD1080p Resolution	Content is supported at HD1080p resolution at 30 fps and 60 fps.
HD H.264 Content and H.264 Content for Cascading links	Enables conference participants to receive higher quality *Content* in both standard conferences and cascaded conferences.
Site Names	Additional controls over the display of site names in the conference Profile.
Interactive Video Forcing	Participants in ongoing conferences can be interactively forced to a Video Window in the conference layout by using Drag and Drop.
Video Preview	H.264 High Profile is supported with Video Preview.
Recording indication	A Recording Indication can be displayed to all conference participants informing them that the conference is being recorded.
Network Quality Indication	A *Network Quality Indicator* is displayed for each participant in the CP layout indicating the quality of the participants' video channels.
Auto scan and Customized Polling	*A* single cell in the conference layout is used to cycle the display of participants that are not in the conference layout. The order of the cyclic display can be predefined.
SirenLPR	Prevents audio degradation and maintains high audio (CD) quality if packet loss occurs.
Speaker Change Threshold	The option to configure the amount of time a participant must speak continuously until becoming the speaker.
Integration with Cisco Telepresence Systems (CTS)	The MCU natively inter-operate with Cisco TelePresence Systems and Polycom TelePresence and vide conferencing endpoints, ensuring optimum quality multi-screen, multipoint calls.
POCN - Collaboration with Microsoft and Cisco in the same environment	The *POCN* solution, enables *Polycom*, *Microsoft* and *Cisco* users, each within their own environment, to participate in the same conference running on an RMX.
Additional Chinese Font Types	Additional Chinese fonts may be selected for several features when using the RMX in Chinese.
Support of Microsoft Protocols, algorithms and workflows	
RTV Video Protocol	Microsoft RTV Video protocol is supported.
RTV B-Frame Support	The MCU supports *Microsoft RTV B-Frame* encoder of real-time video enhancing the viewing experience for *Microsoft Lync* clients. It delivers a better quality video picture by splitting a video frame into pixel segments or slices and predicting the pixel segments in the next video frame.
Conferencing Entities Presence in Microsoft Office Communications Server Client or Lync Server Client	Registration & Presence enables the OCS or LYNC client users to see the availability status (Available, Busy or Offline) of Meeting Rooms, Entry Queues and SIP Factories and connect to them directly from the buddy list.

Table 1-2 *Features Supported with MPMx Card Configuration Mode Only*

Feature Name	**Description**
Cascading between RMX Meeting room / Microsoft A/V MCU	*Microsoft Lync* users can connect an *RMX Meeting Room* to a conference running on the *Microsoft A/V MCU*.
FEC Support	*Support of Microsoft RTV FEC* (*Forward Error Correction*) that controls and correct packet loss when receiving and sending video streams using the *Microsoft Lync Server 2010*.
ICE Over TCP	Enables the automatic usage of the *ICE* connection through the *TCP* port instead of *UDP* when the *UDP* port in the firewall is blocked.
Media Over TCP	Media is automatically transmitted using *TCP* when *UDP*, the default transport protocol, is not available.
Error Recovery	The RMX can automatically recover from short duration network errors (5 seconds), enabling calls in *Microsoft Lync* to continue video or audio conferences without disconnecting.

Workstation Requirements

The *RMX Web Client* and *RMX Manager* applications can be installed in an environment that meets the following requirements:

- **Minimum Hardware** – Intel® Pentium® III, 1 GHz or higher, 1024 MB RAM, 500 MB free disk space.
- **Workstation Operating System** – Microsoft® Windows® XP, Vista®, Windows® 7.
- **Network Card** – 10/100 Mbps.
- **Web Browser** - Microsoft® Internet Explorer® Version 7 or higher.
- RMX Web client and RMX Manager are optimized for display at a resolution of 1280 x 800 pixels and a magnification of 100%.

.Net Framework 2.0 SP1 or above is required and installed automatically.
Internet Explorer must be enabled to allow running Signed ActiveX.
If ActiveX installation is blocked please see the *Polycom® RealPresence® Collaboration Server 1500, 2000, 4000* , "*ActiveX Bypass"* on page **21-69**.

RMX Web Client does not support larger Windows text or font sizes. It is recommended to set the text size to 100% (default) or Normal in the Display settings in Windows Control Panel on all workstations. Otherwise, some dialog boxes might not appear properly aligned. To change the text size, select **Control Panel>Display**. For Windows XP, click the **Appearance** tab, select **Normal** for the Font size and click **OK**. For Windows 7, click the **Smaller - 100%** option and click **OK**.

When installing the *RMX Web Client*, Windows Explorer >Internet Options> Security Settings must be set to *Medium* or less.

It is not recommended to run RMX Web Client and *Polycom CMAD* applications simultaneously on the same workstation.

For Windows 7™ Security Settings, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide*, "*Windows 7™ Security Settings"* on page **1-13**.

For Internet Explorer 8 configuration, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide*, "*Internet Explorer 8 Configuration"* on page **1-14**.

2

Conference Profiles

Profiles stored on the MCU enable you to define all types of conferences. Profiles include conference parameters such as Conferencing Mode, Conference Session Type, Conference Line Rate, People and Content resolution and settings, Video Layout, Encryption, Lost Packet Recovery etc.

The maximum number of *Conference Profiles* that can be defined is:

- RealPresence Collaboration Server (RMX) 1500 - 40
- RealPresence Collaboration Server (RMX) 2000 - 40
- RealPresence Collaboration Server (RMX) 4000 - 80

Conference Profiles are assigned to Conferences, Meeting Rooms, Reservations and Entry Queues. The same *Profile* can be assigned to different conferencing entities. When modifying the *Profile* parameters, the changes will be applied to all the conferencing entities to which the profile is assigned.

Conference Profile options differ according to the selected *Conferencing Mode* and *Conference Type*. Profiles can be defined for AVC (Advanced Video Codec) conferencing Mode or SVC (Scalable Video Codec) conferencing Mode. AVC Conferencing Mode, offers two Video session types: Continuous Presence (CP) conferences and Video Switching (VSW) Conferences. and a special functional conference - Operator Conferences.

Conference Profiles can be saved to *Conference Templates* along with all participant parameters, including their *Personal Layout* and *Video Forcing* settings, enabling administrators and operators to create, save, schedule and activate identical conferences. For more information see Chapter 11, “*Conference Templates*” .

Conferencing Modes

The MCU system offers two Conferencing Modes:

- Transcoding - AVC Conferencing
- Media Relay - SVC Conferencing

Transcoding - AVC Conferencing

In this mode, video is received from all the endpoints using different line rates, different protocols (SIP, H.323, PSTN and ISDN) and video parameters:

- Video protocols: H.261, H.263, H.264 Base and High profile and RTV
- Video Resolutions: from QCIF, CIF and up to 1080p
- Frame rates up to 60 fps

The MCU process the received video, transcodes it and send the resulting video streams to the endpoints. The video processing that is required differs according to the video session set for the conference, with all the processing performed by the MCU. For more details, see "*AVC Conferencing - Video Session Types*" on page **2-2**.

Media Relay - SVC Conferencing

SVC Conferencing is based on the SVC video protocol and SAC audio protocol.

SVC Conferencing offers high resolution video conferencing with low end-to-end latency and improved Error Resiliency without video transcoding by the MCU, hence using less video resources.

The Polycom multipoint media server, acts as an integrated media relay engine that provides media streams for displaying conferences at low latency video experience in video conferences. For more details, see "*SVC-based Conferencing"* on page **2-12**.

AVC Conferencing - Video Session Types

All endpoints have AVC capabilities and can connect to AVC conferences running on the MCU. AVC-based Endpoints can connect can connect using different signaling protocols and different video protocols.

Based on the video processing required during the conference, the RMX offers two *Video Session Types* for *AVC-based conferencing*:

- Continuous Presence
- Video Switching

The video session type determines the video display options (full screen or split screen with all participants viewed simultaneously) and the method in which the video is processed by the MCU (with or without using the MCU's video resources).

Continuous Presence (CP) Conferencing

The dynamic Continuous Presence (CP) capability of the RMX system enables viewing flexibility by offering multiple viewing options and window layouts for video conferencing.

Endpoints can connect to the conference using any signaling protocol (H.323, SIP, ISDN/PSTN and RTV), line rate (up to a maximum line rate defined for the conference), Video Protocol (H.261, H.263, H.264 Base and High Profile) and at any resolution and frame rate (provided they meet the minimum requirements set for the conference).

In Continuous Presence conferences, the MCU receives the video stream from each endpoint at the video rate, video resolution and frame rate that it is capable of sending, and it superimposes all the received streams into one video stream that includes the input from the other endpoints arranges in the selected video layout.

Participants do not see themselves in the video layout. By Default, the speaker is shown in the top left layout cell in symmetric layouts, in the larger cell in asymmetric layouts, or in full screen. The speaker sees the previous speakers (their number depends on the number of cells on the speaker's layout.

The Continuous Presence video session offers layouts to accommodate different numbers of participants and conference settings including support of the VUI annex to the H.264 protocol for endpoints that transmit wide video instead of 4CIF resolution. Each participant can select his/her layout for viewing during the conference, as can be seen in **Figure 2-1**.

For conferences with more participants than display squares, the RMX dynamic video mix capability allows the viewed sites to be modified throughout the conference. The displayed layout can be changed during an ongoing conference, allowing a participant to view different screen layouts of the other conference participants. These layout options allow conferences to have greater flexibility when displaying a large number of participants and maximizes the screen's effectiveness.

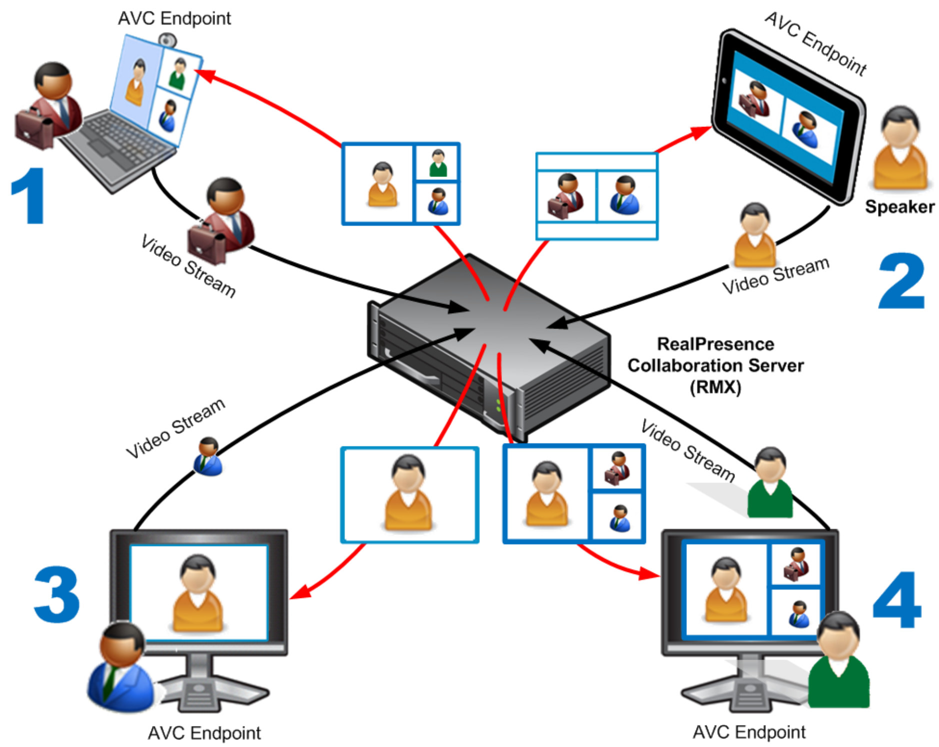


Figure 2-1 AVC Continuous Presence (CP) video streams and built layouts

Video quality in Continuous Presence conferences is affected by the conference line rate (that determines the maximum line rate to be used by the connecting endpoints), and the video capabilities of the endpoints such as the video protocol, video resolution and frame rate. Content sharing is available in all CP conferences.

This requires extensive processing of the video sent to each participant in the conference. The higher the video rate and resolution, the more processing power is required.

By default every conference, Entry Queue and Meeting Room has the ability to declare the maximum CP resolution as defined for the system. This includes conferences launched by the *RMX Web Client* and conferences started via the API.

CP conferencing is defined in the Conference profile by settings the following main features:

- Setting the *Conferencing Mode* to **AVC only**
- Conference Line Rate
- Video Quality – Motion or Sharpness
- Video Layout

Video Protocol Support in CP Conferences

The video protocol selected by the system determines the video compression standard used by the endpoints. In Continuous Presence conferences, the system selects the best video protocol for each of the endpoint according to he endpoint's capabilities.

The following Video protocols are supported in CP conferences:

- **H.261 -** the legacy video compression algorithm mandatory to all endpoints. It is used by endpoints that do not support other protocols.
- **H.263 -** a video compression algorithm that provides a better video quality than H.261. This standard is not supported by all endpoints.
- **H.264** Base Profile **-** a video compression standard that offers improved video quality, especially at line rates lower than 384 Kbps.

  H.264 High Profile allows higher quality video to be transmitted at lower line rates.
- **RTV -** a video protocol that provides high quality video conferencing capability to *Microsoft OCS (Office Communicator Server)* endpoints at resolutions up to *HD720p30*. (SIP only).

Video Switching (VSW) Conferencing

In *Video Switching* mode all participants see the same video picture (full screen). The current speaker is displayed in full screen on all the participants' endpoints, while the speaker sees the previous speaker. Switching between participants is voice-activated; whenever a participant starts to speak, he or she becomes the conference speaker and is viewed on all screens. All conference participants must use the same line rate and video parameters such as video protocol, frame rate, annexes and interlaced video mode as no video processing is performed. Endpoints that are unable to meet these requirements connect as Secondary (audio only).

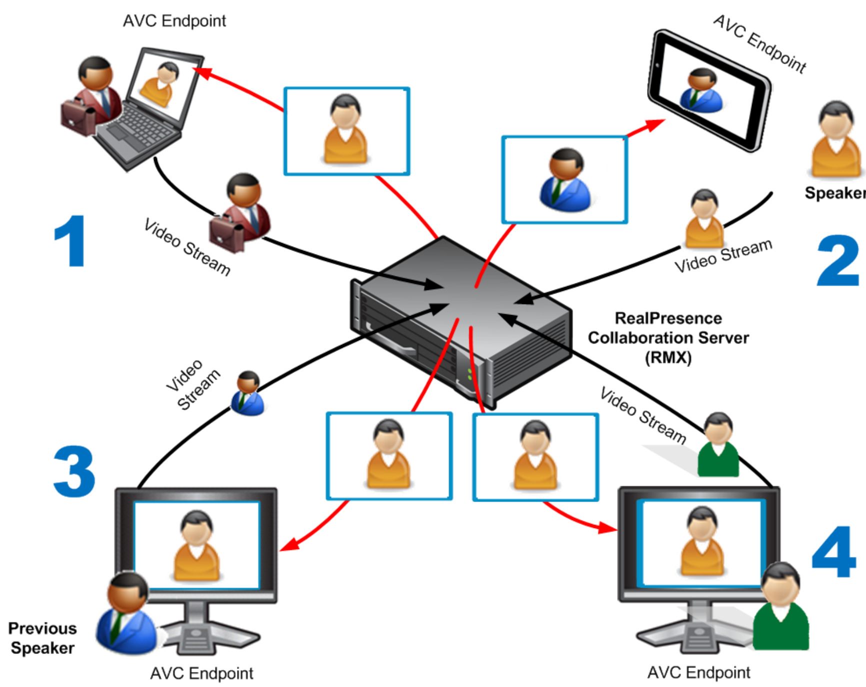


Figure 2-2 *AVC Video Switching (VSW) video streams and Full Screen Layout*

Guidelines

- Only H.264 Base and High Profile video protocols are supported in Video Switching Conferences.
- Video Switching conferences can be set to one of the following resolutions, depending on the capabilities of the endpoints connecting to the conference:
  — H.264 1080p60 (Symmetrically, at bit rates of up to 6Mbps).
  — HD1080p60
  — H.264 1080p30
  — H.264 720p30
  — H.264 720p60
  — H.264 SD 30
  — H.264 CIF (from version 7.6)
  — H.263 CIF (from version 7.6)
  — H.261 CIF (from version 7.6)
- Video Switching conferencing mode is unavailable to ISDN participants.
- Video Switching uses fewer system resources than CP: only one CIF video resource per participant for any resolution (including HD). Table 2-1 lists the resources available to VSW conferences by line rate and card type.

Table 2-1 *VSW Resource Capacity Line Rate*

Resource Type	Maximum Possible Resources Per Card*		
	MPM	MPM+	MPMx
VSW 2Mbps	40	80	80*
VSW 4Mbps	40	40	40*
VSW 6Mbps	-	20	20*

* Capacity numbers are for maximum capacity card assemblies. These numbers may be lower when LPR and/or encryption are enabled.

Table 2-2 lists the recommended number of connections at *HD1080p* resolution for fully configured and licenced RealPresence Collaboration Server (RMX) systems with MPMx cards. For detailed resource capacity information see the relevant RMX Hardware Guide.

Table 2-2 *Maximum Number of HD1080p Connections by Line Rate*

Line Rate/Participants	RMX 1500	RMX 2000	RMX 4000
Up to 2Mbps	80	160	320
4Mbps	40	80	160
6Mbps **(MPM+/MPMx)**	20	40	80

- The maximum supported video conference size is 160 participants with the MPM+ card and 180 participants with the MPMx card.
- The display aspect ratio is 4x3 or 16x9.

- Site (endpoint) names, skins, message overlay etc. are not supported in Video Switching.
- Video forcing is enabled at the conference and participant levels.
- To connect to a Video Switching conference via Entry Queue, the *Profile* assigned to the Entry Queue must be set to Video Switching. It is recommended to use the same profile for both the destination conference and Entry Queue.
- The *HD_THRESHOLD_BITRATE* flag must be set in the *System Configuration*. The value of this flag is the **system** minimum threshold bit rate for HD resolutions. The line rate selected in the conference Profile must be the same as or higher than that specified by the *HD_THRESHOLD_BITRATE* flag.

The HD_THRESHOLD_BIT RATE flag is responsible for negotiation only, It does not guarantee that the endpoint will open an HD channel or transmit on an opened HD channel.

The **HD_THRESHOLD_BITRATE** flag line rate value ranges from 384kbps to 4Mbs, default is 768kbps. For more information, see "*Modifying System Flags"* on page **22-1**.

Line Rates for CP and VSW

Table 2-3 lists the video session modes available at all supported line rates in MPM, MPM+ and MPMx card configuration modes.

Table 2-3 *Video Session Mode by Line Rate and Card type*

<table>
<tr><th>Line Rate (kbps)</th><th>MPM</th><th>MPM+</th><th>MPMx</th></tr>
<tr><td>64</td><td rowspan="18">CP / Video Switching</td><td>CP / Video Switching</td><td>CP / Video Switching</td></tr>
<tr><td>96</td><td></td><td></td></tr>
<tr><td>128</td><td></td><td></td></tr>
<tr><td>192</td><td></td><td></td></tr>
<tr><td>256</td><td></td><td></td></tr>
<tr><td>320</td><td></td><td></td></tr>
<tr><td>384</td><td></td><td></td></tr>
<tr><td>512</td><td></td><td></td></tr>
<tr><td>768</td><td></td><td></td></tr>
<tr><td>832</td><td></td><td></td></tr>
<tr><td>1024</td><td></td><td></td></tr>
<tr><td>1152</td><td></td><td></td></tr>
<tr><td>1280</td><td></td><td></td></tr>
<tr><td>1472</td><td></td><td></td></tr>
<tr><td>1536</td><td></td><td></td></tr>
<tr><td>1728</td><td></td><td></td></tr>
<tr><td>1920</td><td></td><td></td></tr>
<tr><td>2048</td><td></td><td></td></tr>
</table>

Table 2-3 Video Session Mode by Line Rate and Card type (Continued)

Line Rate (kbps)	MPM	MPM+	MPMx
2560	Video Switching		
3072			
3584			
4096			
6144	Not Supported		Video Switching

AVC Conferencing Parameters

Basic Conferencing Parameters

When defining a new video Profile, you select the parameters that determine the video display on the participant's endpoint and the quality of the video. When defining a new conference Profile, the system uses default values for Continuous Presence (CP) standard conferencing. Continuous Presence conferencing enables several participants to be viewed simultaneously and each connected endpoint uses its highest video, audio and data capabilities up to the maximum line rate set for the conference.

The main parameters that define the quality of a video conference are:

- **Line (Bit) Rate -** The transfer rate of video and audio streams. The higher the line (bit) rate, the better the video quality.
- **Audio Algorithm -** The audio compression algorithm determines the quality of the conference audio.
- **Video protocol, video format, frame rate, annexes, and interlaced video mode** - These parameters define the quality of the video images. The RMX will send video at the best possible resolution supported by endpoints regardless of the resolution received from the endpoints.
  - — When *Sharpness* is selected as the *Video Quality* setting in the *Conference Profile*, the RMX will send 4CIF (H.263) at 15fps instead of CIF (H.264) at 30fps.
  - — *H.264 High Profile* protocol provides better compression of video images in line rates lower than 384 Kbps and it will be automatically selected for the endpoint if it supports H.264 *High Profile*. If the endpoint does not support H.264 High Profile, the RMX will try H.264 Base Profile which provides good compression of video images in line rates lower than 384 Kbps (better than H.263 and not as good as H.264 *High Profile).*
  - — When working with RMXs at low bit rates (128, 256, or 384Kbps), HDX endpoints will transmit SD15 resolution instead of 2CIF resolution.

  When using a full screen (1x1) conference layout, the RMX transmits the same resolution it receives from the endpoint.
- **Lost Packet Recovery (LPR) -** LPR creates additional packets that contain recovery information used to reconstruct packets that are lost during transmission.

- **Video Clarity** - Video Clarity feature applies video enhancing algorithms to incoming video streams of resolutions up to and including SD.
- Supported resolutions:
  - **H.261 CIF/QCIF –** Is supported in Continuous Presence (CP) conferences at resolutions of 288 x 352 pixels (CIF) and 144 x 176 pixels (QCIF). Both resolutions are supported at frame rates of up to 30 frames per second.
  - **H.263 4CIF** - A high video resolution available to H.263 endpoints that do not support H.264. It is only supported for conferences in which the video quality is set to sharpness and for lines rates of 384kbps to 1920kbps.
  - **Standard Definition (SD)** - A high quality video protocol which uses the H.264 and H.264 High Profile video algorithms. It enables compliant endpoints to connect to Continuous Presence conferences at resolutions of 720X576 pixels for PAL systems and 720X480 pixels for NTSC systems. For more information, see "*Video Resolutions in AVC-based CP Conferencing"* on page **3-1**.
  - **High Definition (HD)** – HD is an ultra-high quality video resolution that uses he H.264 and H.264 High Profile video algorithms. Depending on the RMX's Card Configuration mode compliant endpoints are able to connect to conferences at the following resolutions:
    - **720p** (1280 x 720 pixels) in MPM, MPM+ and MPMx Card Configuration Modes
    - **1080p** (1920 x 1080 pixels) in MPM+ and MPMx Card Configuration Modes

    For more information, see "*Video Resolutions in AVC-based CP Conferencing"* on page **3-1**.

From *Version 7.1*, *MPM* media cards are not supported.

Supplemental Conferencing Features

In addition to *Standard Conferencing* the following features can be enabled:

- **H.239 –** Allows compliant endpoints to transmit and receive two simultaneous streams of conference data to enable Content sharing. H.239 is also supported in cascading conferences. Both H.263 and H.264 Content sharing protocols are supported. If all endpoints connected to the conference have H.264 capability, Content is shared using H.264, otherwise Content is shared using H.263.
  For more information, see **"***H.239"* **on page 4-2.**
- **Lecture Mode –** The lecturer is seen by all participants in full screen while the lecturer views all conference participants in the selected video layout.
  For more information, see **"***Lecture Mode (AVC Only)"* **on page 4-73.**
- **Presentation Mode (CP Conferences only) –** When the current speaker's speech exceeds a predefined time (30 seconds), the conference layout automatically changes to full screen, displaying the current speaker as the conference lecturer on all the participants' endpoints. During this time the speaker's endpoint displays the previous conference layout. When another participant starts talking, the Presentation Mode is cancelled and the conference returns to its predefined video layout. Presentation mode is available with *Auto Layout* and *Same Layout.*
  - If the speaker in a video conference is an Audio Only participant, the Presentation Mode is disabled for that participant.

- — Video forcing works in the same way as in Lecture Mode when Presentation Mode is activated, that is, forcing is only enabled at the conference level, and it only applies to the video layout viewed by the lecturer.
- **Telepresence Mode (CP Conferences only) -** enables the connection of numerous high definition telepresence rooms and of different models (such as TPX and RPX) into one conference maintaining the telepresence experience. This mode is enabled by a special license.
- **Encryption –** Used to enhance media security at conference and participant levels. For more information, see "*Audio Algorithm Support"* on page **4-35**.
- **Conference Recording -** The RMX enables audio and video recording of conferences using Polycom RSS 2000 recording system.
- **Packet Loss Concealment (PLC) -** for *Siren* audio algorithms improves received audio when packet loss occurs in the network. *PLC* is enabled by the **SET_AUDIO_PLC** *System Flag* in *system.cfg*
  - — *PLC for Audio* is supported with *MPM*+ and MPMx cards only.
  - — The speaker's endpoint must use a *Siren* algorithm for audio compression.
  - — The following audio algorithms are supported:
    - *Siren 7* (mono)
    - *Siren 14* (mono/stereo)
    - *Siren 22* (mono/stereo)
- **Auto Brightness -** detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout.
  - — *Auto Brightness* is supported with *MPM+ and MPMx* cards only.
  - — *Auto Brightness* only increases brightness and does not darken video windows.
- **Audio Clarity -** improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity.
  - — *Audio Clarity* is supported with *MPM*+ and *MPMx* cards only.
  - — *Audio Clarity* is applied to the following low bandwidth (4kHz) audio algorithms:
    - G.729a
    - G.711

TIP Support

TIP is a proprietary protocol created by *Cisco* for deployment in *Cisco TelePresence systems (CTS)*. *Polycom's* solution is to allow the RMX to natively inter-operate with *Cisco TelePresence Systems*, ensuring optimum quality multi-screen, multipoint calls. For more information, see "*Collaboration With Cisco's Telepresence Interoperability Protocol (TIP)"* on page **I-1**.

Operator Conferences (CP only Conferences)

Offers additional conference management capabilities to the RMX users, enabling them to attend to participants with special requirements and acquire participant details for billing and statistics. This service is designed usually for large conferences that require the personal touch. Operator assistance is available in MPM, MPM+ and MPMx *Card Configuration Modes*. For more information, see Chapter 10, "*Operator Assistance & Participant Move"* on page **10-1**

Default Profile Settings in CP Conferencing Mode

The RMX is shipped with a default *Conference Profile* for CP conferences which allows users to immediately start standard ongoing CP conferences. These are also the default settings when creating a new Profile. The default settings are as follows:

Table 2-4 *Default Conference Profile Settings (CP Licensing Mode)*

Setting	Value
Profile Name	Factory Video Profile
Line Rate	384Kbps
Video Switching	Disabled
Operator Conference	Disabled
Encryption	Disabled
Packet Loss Compensation (LPR and DBA)	Enabled for CP Conferences
Auto Terminate	• After last participant quits - Enabled • When last participant remains - Disabled
Auto Redialing	Disabled
Exclusive Content Mode	Disabled
TIP Compatibility	Disabled
Enable FECC	Enabled
Enabled Gathering Phase	Enabled
Display Language	English
Video Quality	Sharpness
Maximum Resolution	Auto
Video Clarity	Enabled
Auto Brightness	Enabled
Content Settings	Graphics
Content Protocol	H.263 & H.264 Auto Selection
Presentation Mode	Disabled
Send Content to legacy endpoints	Disabled
Same Layout	Disabled
Lecturer View Switching	Disabled
Telepresence Mode	Auto
Telepresence Layout Mode	Continuous Presence

Table 2-4 *Default Conference Profile Settings (CP Licensing Mode) (Continued)*

Setting	Value
Auto Scan Interval	Disabled (10)
Auto Layout	Enabled
Echo Suppression	Enabled
Keyboard Noise Suppression	Disabled
Audio Clarity	Enabled
Mute participants except the lecturer	Disabled
Skin	Polycom
IVR Name	Conference IVR Service
Recording	Disabled
Site Names display	Disabled
Message Overlay	Disabled
Network Services - SIP Registration	Disabled
Network Services - Accept Calls	Enabled

This *Profile* is automatically assigned to the following conferencing entities:

Name	ID
Meeting Rooms	
Maple_Room	*1001*
Oak_Room	*1002*
Juniper_Room	*1003*
Fig_Room	*1004*
Entry Queue	
Default EQ	*1000*

SVC-based Conferencing

The SVC-Based conferencing mode provides video without transcoding by the MCU, hence requiring less video resources while providing better error resiliency and lower latency.

Using the SVC video protocol, SVC conferences provide video bit streams at different resolutions, frame rates and line rates to SVC-enabled endpoints with various display capabilities and layout configurations.

In the SVC-based conference, each SVC-enabled endpoint transmits multiple bit streams, called simulcasting, to the Polycom® RealPresence® Collaboration Server. Simulcasting enables each endpoint to transmit at different resolutions and frame rates such as 720p at 30fps, 15fps, and 7.5fps, 360p at 15fps and 7.5fps, and 180p at 7.5fps.

The Polycom SVC-enabled endpoints (such as Polycom® RealPresence® Desktop and Polycom® RealPresence® Mobile) compose the layout according to their layout settings and video capabilities. This enables the MCU to send or relay the selected video streams to each endpoint without processing the video streams and sending the composite video layout to the endpoints.

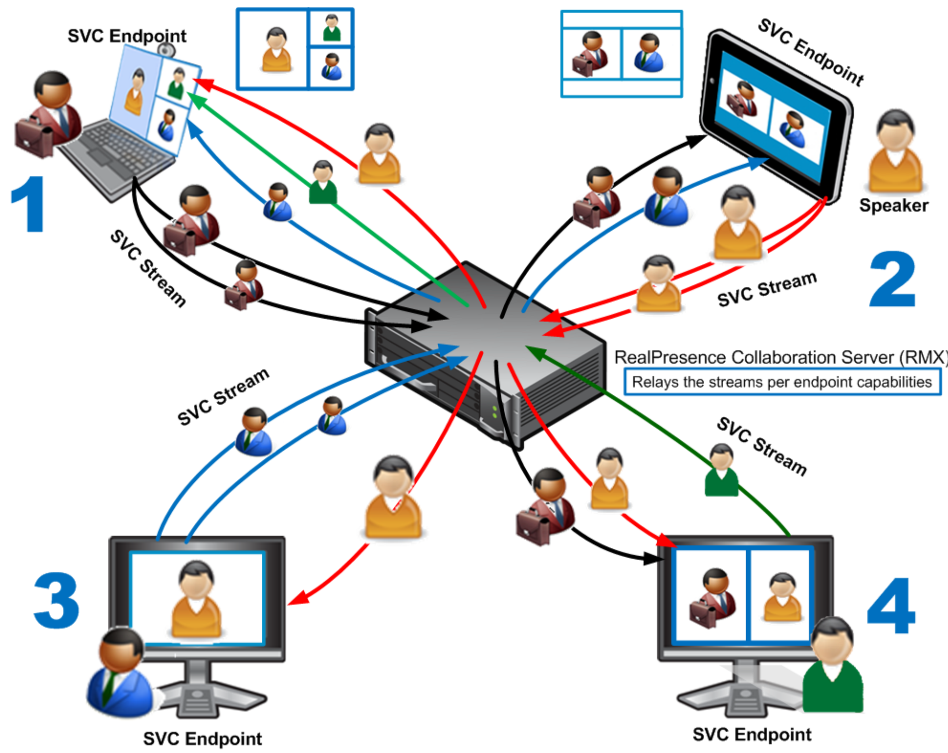


Figure 2-3 *SVC video streams and Layouts*

The video streams displayed in the conference layout on each endpoint is obtained from the different streams received from each of the endpoints displayed in the layout. Depending on the size of the video cell in the configured layout, the endpoint requests the video stream in the required resolution from the RealPresence Collaboration Server. The higher the display quality and size, the higher the requested resolution will be sent to the endpoint. The endpoint creates the displayed layout from the different video streams it receives.

For instance, an SVC endpoint might want to receive three video streams at different frame rates and resolutions, and create a conference layout with the received video streams. Each SVC-enabled endpoint sends encoded SVC bit streams to the MCU to relay to the other SVC-enabled endpoints in the conference.

The endpoints encode the video in multiple resolutions and decodes the multiple video input streams.

For example:

RealPresence mobile client (**2**) will transmit two resolutions; one that is suited for RealPresence Desktop client (**3**) and a second that is suited for two other endpoints: RealPresence Desktop client (**4**) and (**1**).

RealPresence Desktop client (**1**) transmits two resolutions; one that is suited for RealPresence Mobile client (**2**) and a second that is suited for RealPresence Desktop client (**4**).

The MCU determines which of the incoming resolutions to send to each endpoint. It does not perform any SVC encoding and decoding, or any transcoding of the video streams. The RealPresence Collaboration Server functions as the multipoint media relay to the endpoints. For voice activated selection of the video streams, the RealPresence Collaboration Server determines which of the incoming bit streams to send to each endpoint.

Advantages of SVC Conferencing

SVC increases the scalability of video networks and enables mass desktop video deployments. Some of the advantages of SVC conferencing are:

- Offers high-resolution video conferencing with low end-to-end latency, improved error resiliency and higher system capacities.
- Allows the SVC-enabled video endpoints to manage display layouts, supporting multiple line rates, resolutions and frame rates.
- The RealPresence Collaboration Server functions as a media relay server providing low cost production benefits. The RealPresence Collaboration Server reduces bandwidth usage by only selecting the necessary video stream to be sent to the endpoints.

Guidelines

- SVC conferences are supported only with the following:
  - RMX systems with MPMx card
  - CP Licensing
  - SIP over UDP signaling
  - SIP over TLS Signaling
  - Polycom SVC-enabled endpoints (Polycom® RealPresence® Desktop, Polycom® RealPresence® Mobile)
  - Ad Hoc conferencing via Meeting Rooms and ongoing conferences
- SVC Only conferences can run on the same MCU as AVC Only conferences.
- All the endpoints participating in a single SVC Only conference must be connected to the same media card and cannot be handled by different media cards as the SVC media streams cannot be shared between them.
- End-to-end latency on a local network (same site), is around 200mSec to ensure AV sync (also known as Lip-sync).
- Dial-out is not available in SVC Only conference.

- Dial-in is available as follows:
  - AVC endpoints (participants) can only connect to an AVC conference. When dialing into SVC Only conferences they will be disconnected and the calls fail.
  - SVC endpoints support both AVC and SVC video protocols.
    When dialing into SVC Only conferences, they connect as SVC endpoints.
    When dialing into AVC Only conferences, they connect as AVC endpoints. They cannot connect to an AVC conference using the SVC capabilities.
- SVC endpoints cannot connect to SVC Only conferences via Entry Queues.
- SVC endpoints cannot be moved between conferences.
- Content is supported in H.264 (AVC).
  - Only the *H.264 Cascade and SVC Optimized* option is supported.
  - LPR and DBA are not supported for SVC content sharing.
- Auto Layout is the default and only setting to display the video on the endpoint screen.
- Site names display is controlled from the SVC endpoints.
- When DMA is part of the solution, the DMA is used as the SIP proxy and the SVC endpoint subscribes to DMA for call control. If a DMA is not part of the solution, the SVC endpoint dial directly to the RMX using IP addresses is the SIP dialing strings.
- When Hot backup is enabled, all the conferences are created on the Slave MCU.
- When Hot Backup is activated and the Slave MCU becomes the Master MCU:
  - All AVC endpoints will be reconnected to the AVC (CP and VSW) conferences. SVC endpoints connected to AVC conferences using their AVC capabilities will be reconnected to their AVC conferences.
  - SVC endpoints cannot be reconnected to their SVC Only conferences as dial-out is not supported for SVC endpoints. These endpoints will have to manually reconnect to their SVC conferences.
- Cascading between SVC Only conferences or between AVC and SVC Only conferences is not supported.
- Gateway sessions are not supported for SVC calls.
- Reservations cannot be scheduled for SVC Only conferences.
- The following functionality and features are not supported during SVC Only conferences:
  - FECC
  - Skins. The video cells are displayed on the endpoint's default background.
  - IVR functionality
  - Conference Gathering phase
  - Password protected conferences as DTMF input for passwords cannot be processed
  - All DTMF enabled features during the conference
  - Manual selection of video layout
  - Chairperson functionality
  - Media Encryption
  - Recording of SVC Only conferences
  - Text messaging using Message Overlay

MCU Supported Resolutions for SVC Conferencing

The MCU automatically selects the resolution and frame rate according to the conference line rate. Table 2-5 details the maximum resolution and frame rates supported by the MCU for each conference line rate. The actual video rate, resolution and frame rates displayed on each endpoints is determined by the endpoint's capabilities.:

Table 2-5 *SVC Conferencing - Maximum Supported Resolutions per Simulcast Stream*

Conference Line Rate (kbps)	Profile	Maximum Resolution	Max. Frame Rate (fps)	Audio Rate (kbps)
1472 - 2048	High Profile	720p	30fps	48
1024 - 1472	High Profile	720p	15fps	48
768 - 1024	High Profile	360p	30fps	48
512 - 768	High Profile	360p	15fps	48
256 - 512	Base Profile	180p	30fps	48
192 - 256	Base Profile	180p	15fps	48
128 - 192	Base Profile	180p	7.5fps	48

Viewing Profiles

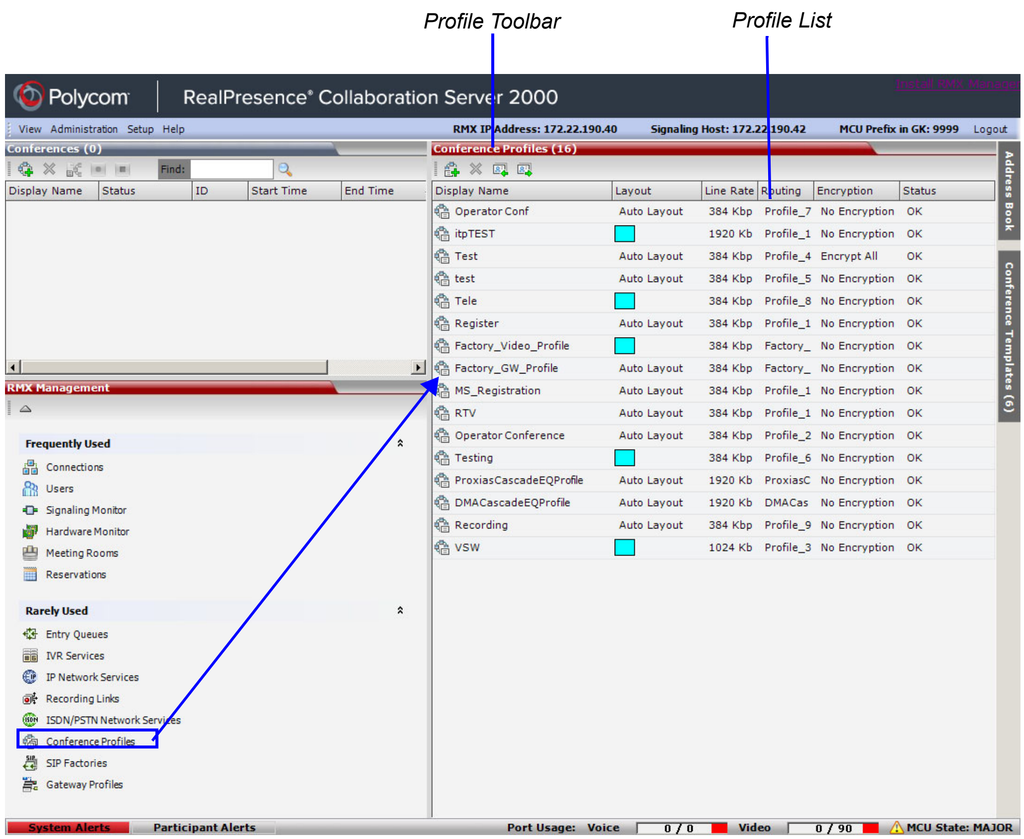
Conference Profiles are listed in the *Conference Profiles* list pane.

To list Conference Profiles:

1 In the *RMX Management* pane, expand the *Rarely Used* list.

2 Click the **Conference Profiles** button.

The *Conference Profiles* are displayed in the *List* pane.



The number of the currently defined Conference Profiles appears in the title of the list pane.

The following *Conference Profile* properties are displayed in the *List* pane:

Table 2-6 *Conference Profiles Pane Columns*

Field	Description
Name	The name of the *Conference Profile*.
Layout	Displays either "*Auto Layout*" or an icon of the layout selected for the profile. For information about video layouts, see Table 2-14 "*Video Layout Options"* on page **2-34**.
Line Rate	The maximum bit rate in kbps at which endpoints can connect to the conference.

Table 2-6 Conference Profiles Pane Columns (Continued)

Field	Description
Routing Name	Displays the Routing Name defined by the user or automatically generated by the system.
Encryption	Displays if media encryption is enabled for the Profile. For more information see "*Media Encryption (AVC Only)"* on page **4-40**.

Profile Toolbar

The Profile toolbar provides quick access to the Profile functions:

Table 2-7 Profile Tool bar buttons

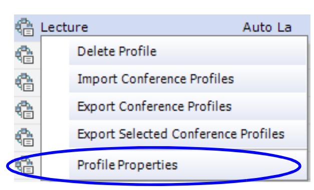
Button	Button Name	Description
	*New Profile*	To create a new Profile.
	*Delete Profile*	To delete a Profile, click the Profile name and then click this button.
	*Import Profile*	To import Conference Profiles from another MCU in your environment.
	*Export Profile*	To export Conference Profiles to a single XML file that can be used to import the Conference Profiles on multiple MCUs.

Modifying an Existing Profile

You can modify any of the Profile's parameters but you cannot rename the *Profile*.

To modify the Profile Properties:

1 In the *Conference Profiles* list, double -click the *Profile* icon or right-click the *Profile* icon, and then click **Profile Properties**.



The Profile *Properties - General* dialog box opens.

Deleting a Conference Profile

To delete a Conference Profile:

1 In the *Conference Profiles* list, select the *Conference Profile* you want to delete.

2 Click the **Delete Profile** ( ) button.
or
Right-click the *Conference Profile* to be deleted and select **Delete Profile** from the drop-down menu.

A confirmation dialog box is displayed.

3 Click **OK** in the confirmation dialog box.

4 The *Conference Profile* is deleted.

> A *Conference Profile* cannot be deleted if it is being used by Meeting Rooms, Entry Queues, SIP Factories and Reservations.
> A Profile that is assigned to only one ongoing conference and no other conferencing entity can be deleted.

Defining New Profiles

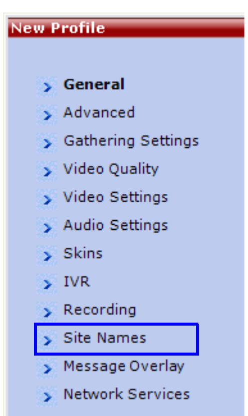
Conference Profile options differ according to the selected *Conferencing Mode* and *Conference Type*. Profiles can be defined for AVC (Advanced Video Codec) conferencing Mode or SVC (Scalable Video Codec) conferencing Mode. AVC Conferencing Mode, offers two Video session types: Continuous Presence (CP) conferences and Video Switching (VSW) Conferences. and a special functional conference - Operator Conferences.

Profiles are the basis for the definition of all ongoing conferences, *Reservations*, *Meeting Rooms*, *Entry Queues*, and *Conference Templates* and they contain only conference properties.

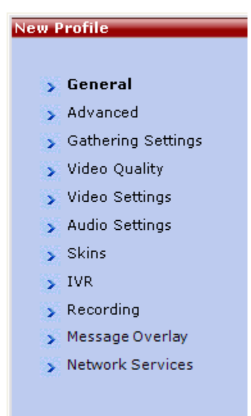
The tabs displayed in the *New Profile* dialog box are dependent on the *Card Configuration Mode* of the *RMX* – whether the RMX is configured with *MPMx* or *MPM+* cards.

In *MPMx Mode*, an additional tab - *Site Names* is displayed:

MPMx



MPM+



In *MPM+ Card Configuration Mode*, the Site Names are configured and behave as in version 7.6 and earlier.

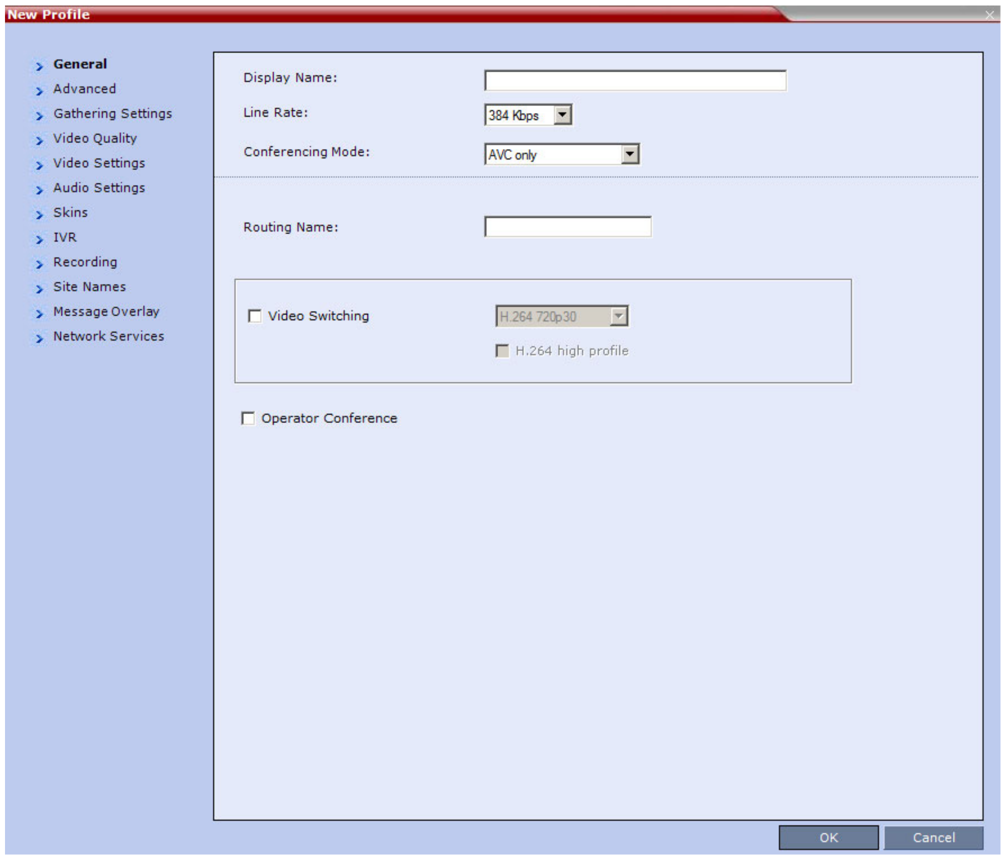
The following *Profile Definition* procedure assumes that the RMX is in *MPMx Mode*. Differences in the procedure that are affected by the *Card Configuration Mode* will be highlighted and explained as and when applicable.

Defining AVC Conferencing Profiles

To define a new Profile:

1 In the *RMX Management* pane, click **Conference Profiles**.

2 In the *Conference Profiles* pane, click the **New Profile** button.
The *New Profile – General* dialog box opens.



3 Define the *Profile* name and, if required, the *Profile - General* parameters:

Table 2-8 New AVC Profile - General Parameters

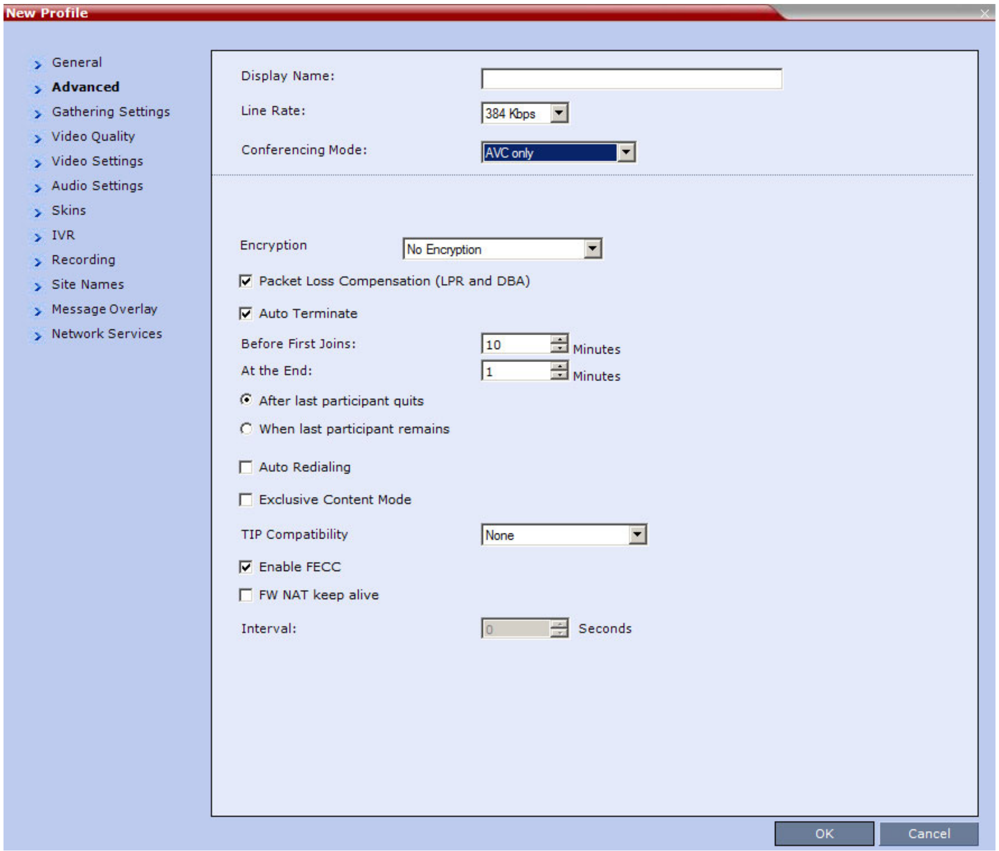
Field/Option	Description
Display Name	Enter a unique Profile name, as follows: • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. It is recommended to use a name that indicates the Profile type, such as Operator conference or Video Switching conference. **Note:** This is the only parameter that must be defined when creating a new profile. **Note:** This field is displayed in all tabs.
Line Rate	Select the conference bit rate. The line rate represents the combined video, audio and Content rate. The default setting is 384 Kbps. **Notes:** • This field is displayed in all tabs. • Maximum line rate at which ISDN endpoints can connect to a conference is 768 kbps.
Conferencing Mode	Foe AVC conferencing, make sure that **AVC Only** (default) is selected to define a CP or VSW conference Profile. **Note:** This field is displayed in all tabs.
Routing Name	Enter the *Profile* name using ASCII characters set. The Routing Name can be defined by the user or automatically generated by the system if no Routing Name is entered as follows: • If an all ASCII text is entered in Display Name, it is used also as the Routing Name. • If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name.

Table 2-8 *New AVC Profile - General Parameters (Continued)*

Field/Option	Description
Video Switching	If the *Operator Conference* option is selected, this option is disabled, and the selection is cleared. Select the video protocol and resolution for the conference. When selected, the conference is in a special conferencing mode which implies that all participants must connect at the same line rate and use the same video resolution. Participants with endpoints that do not support the selected line rate and resolution will connect as secondary (audio only). For more information, see "*Video Switching (VSW) Conferencing"* on page **2-4**. **Notes:** • Video Switching conferencing mode is unavailable to ISDN participants. • To connect to a Video Switching conference via Entry Queue, the Profile assigned to the Entry Queue must be set to Video Switching. It is recommended to use the same profile for both the destination conference and Entry Queue. • *Telepresence Mode* is unavailable in *Video Switching* conferences.
H.264 High Profile	Select this check box to enable the use of *H.264 High Profile* in *Video Switching* conferences. For more information, see *"H.264 High Profile Support in Video Switching Conferences"* on page **2-53**.
Operator Conference ***(CP Only)***	Select this option to define the profile of an Operator conference. An Operator conference can only be a Continuous Presence conference, therefore when selected, the *Video Switching* option is disabled and cleared. When defining an *Operator Conference*, the *Send Content to Legacy Endpoints* option in the *Video Settings* tab is cleared and disabled. For more information, see Chapter 10, "*Operator Assistance & Participant Move"* on page **10-1**.

4 Click the **Advanced** tab.

The *New Profile – Advanced* dialog box opens.



5 Define the following parameters:

Table 2-9 *New AVC Profile - Advanced Parameters*

Field/Option	Description
Encryption	Select the Encryption option for the conference: • **Encrypt All** - Encryption is enabled for the conference and all conference participants must be encrypted. • **No Encryption** - Encryption is disabled for the conference. • **Encrypt when Possible** - enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. For connection guidelines see "*Mixing Encrypted and Non-encrypted Endpoints in one Conference”* on page **4-41**. For more information, see "*Media Encryption (AVC Only)”* on page **4-40**.

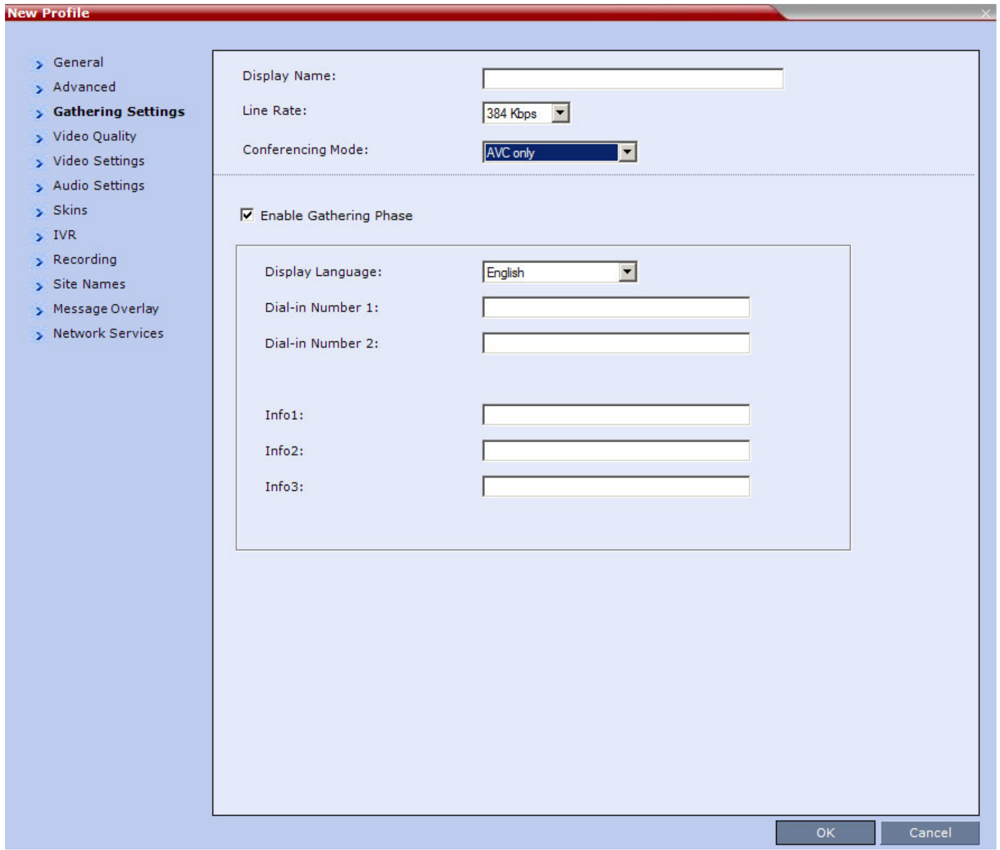
Table 2-9 *New AVC Profile - Advanced Parameters (Continued)*

Field/Option	Description
LPR	When selected (default for CP conferences), *Lost Packet Recovery* creates additional packets that contain recovery information used to reconstruct packets that are lost during transmission. LPR check box is automatically cleared if *High Definition Video Switching* is selected, but can be selected if required. For more information, see "*Packet Loss Compensation (LPR and DBA)"* on page **4-50**.
Auto Terminate	When selected (default), the conference automatically ends when the termination conditions are met: ***Before First Joins*** — No participant has connected to a conference during the *n* minutes after it started. Default idle time is 10 minutes. ***At the End - After Last Quits*** — All the participants have disconnected from the conference and the conference is idle (empty) for the predefined time period. Default idle time is 1 minute. ***At the End - When Last Participant Remains*** — Only one participant is still connected to the conference for the predefined time period (excluding the recording link which is not considered a participant when this option is selected). This option should be selected when defining a Profile that will be used for Gateway Calls and you want to ensure that the call is automatically terminated when only one participant is connected. Default idle time is 1 minute. **Note:** The selection of this option is automatically cleared and disabled when the *Operator Conference* option is selected. The Operator conference cannot automatically end unless it is terminated by the RMX User.
Auto Redialing	The *Auto Redialing* option instructs the RMX to automatically redial *IP* and *SIP* participants that have been abnormally disconnected from the conference. • *Auto Redialing* is disabled by default. • *Auto Redialing* can be enabled or disabled during an ongoing conference using the Conference Properties – Advanced dialog box. • The RMX will not redial an endpoint that has been disconnected from the conference by the participant. • The RMX will not redial an endpoint that has been disconnected or deleted from the conference by an operator or administrator.
Exclusive Content Mode	Select the *Exclusive Content Mode* check box to limit the Content broadcasting to one participant, preventing other participants from interrupting the Content broadcasting while it is active. For more details, see "*Exclusive Content Mode"* on page **4-21**.

Table 2-9 *New AVC Profile - Advanced Parameters (Continued)*

Field/Option	Description
TIP Compatibility	Select the *TIP Compatibility* mode when implementing an *RMX and Cisco Telepresence Systems (CTS) Integration* solution. • None • Video Only • Video & Content The *TIP Compatibility* mode affects in the user video and content experience. For more information, see "*Collaboration With Cisco's Telepresence Interoperability Protocol (TIP)"* on page **I-1**.
Enable FECC	This option is enabled by default, allowing participants in the conference to control the zoom and PAN of other endpoints in the conference via the FECC channel. Clear this check box to disable this option for all conference participants.
FW NAT Keep Alive	The RMX can be configured to send a *FW NAT Keep Alive* message at specific Intervals for the *RTP*, *UDP* and *BFCP* channels. For more information see "*FW (Firewall) NAT Keep Alive"* on page **16-74**.
Interval	If needed modify the *NAT Keep Alive Interval* field within the range of 5 - 86400 seconds.For more information see "*FW (Firewall) NAT Keep Alive"* on page **16-74**.

6 **For CP Conferences only:** Click the **Gathering Settings** tab.



7 **Optional.** Define the following fields if the conference is not launched by the *Polycom Conferencing Add-in for Microsoft Outlook*:

- If the conference is launched by the *Polycom Conferencing Add-in for Microsoft Outlook* the field information is received from the meeting invitation and existing field value are overridden. For more information see "*Polycom Conferencing for Microsoft Outlook®"* on page **12-1**.
- From Version 7.2, the Gathering option is disabled in gateway calls.

Table 2-10 New AVC Profile - Gathering Settings Parameters

Field	Description
Display Name	This field is defined when the *Profile* is created. For more information see the "*Defining New Profiles"* on page **2-18**.
Enable Gathering	Select this check box to enable the *Gathering Phase* feature. Default: Selected.

Table 2-10 *New AVC Profile - Gathering Settings Parameters*

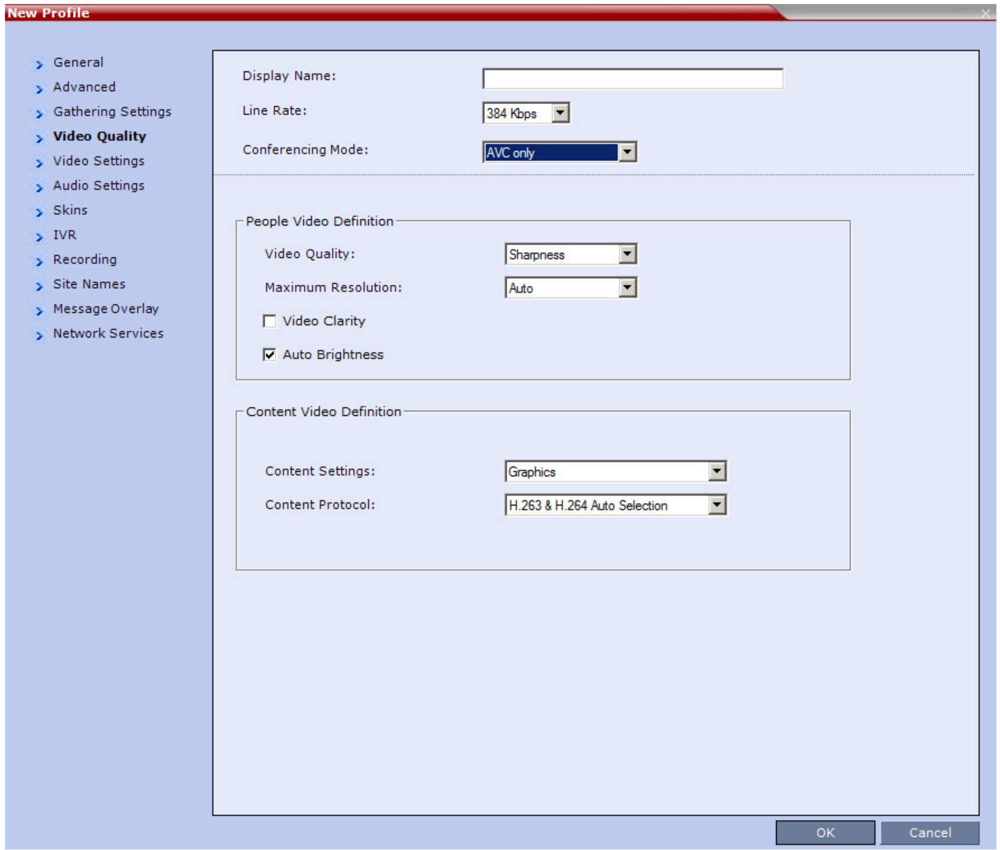
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Displayed Language</td><td>Select the Gathering Phase slide language:
Gathering Phase slide field headings are displayed in the language selected.
The Gathering Phase slide can be in a different language to the RMX Web Client.
Default: English
Note: When working with the Polycom Conferencing Add-in for Microsoft Outlook, the language selected should match the language selected for the conference in the Polycom Conferencing Add-in for Microsoft Outlook to ensure that the Gathering Phase slide displays correctly.</td></tr>
<tr><td>Access Number 1</td><td rowspan="2">Enter the ISDN or PSTN number(s) to call to connect to the conference.
Note: The numbers entered must be verified as the actual Access Numbers.</td></tr>
<tr><td>Access Number 2</td></tr>
<tr><td>Info 1</td><td rowspan="3">Optionally, enter any additional information to be displayed during the Gathering Phase.
These fields are not limited in the RMX Web Client but only 96 characters can be displayed in the Gathering Slide on a 16:9 monitor.
If the Gathering slide is displayed on a 4:3 endpoint: the slide is cropped on both sides:
• The left most characters of the information fields are not displayed.
• The live video is cropped on the right side of the display.
Info 1
Info 2
Info 3

</td></tr>
<tr><td>Info 2</td></tr>
<tr><td>Info 3</td></tr>
</table>

For more information see "*Video Preview"* on page **4-26**.

8 Click the **Video Quality** tab.

The *New Profile – Video Quality* dialog box opens.



9 Define the following parameters:

Table 2-11 *New AVC Profile - Video Quality Parameters*

Field/Option	Description
People Video Definition	
Video Quality	Depending on the amount of movement contained in the conference video, select either: • ***Motion*** – for a higher frame rate without increased resolution. When selected, *Video Clarity* is disabled. • ***Sharpness*** – for higher video resolution and requires more system resources. **Note:** When Sharpness is selected as the *Video Quality* setting in the conference Profile, the RMX will send 4CIF (H.263) at 15fps instead of CIF (H.264) at 30fps. For more information, see "*Video Resolutions in AVC-based CP Conferencing"* on page **3-1**.

Table 2-11 New AVC Profile - Video Quality Parameters (Continued)

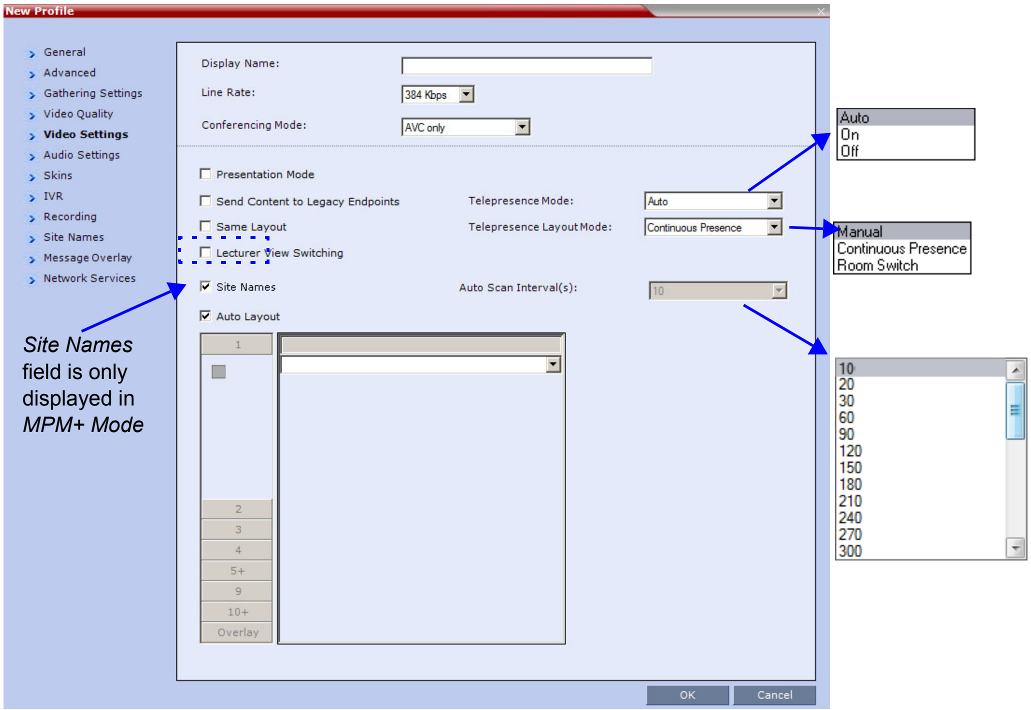
Field/Option	Description
Maximum Resolution	This setting overrides the *Maximum Resolution* setting of the *Resolution Configuration* dialog box. The administrator can select one of the following *Maximum Resolution* options: • *Auto* (default) - The *Maximum Resolution* remains as selected in the *Resolution Configuration* dialog box. • *CIF* • *SD* • *HD720* • *HD1080* *Maximum Resolution* settings can be monitored in the *Profile Properties - Video Quality* and *Participant Properties - Advanced* dialog boxes. **Notes:** The *Resolution* field in the *New Participant - Advanced* dialog box allows *Maximum Resolution* to be **further limited** per participant endpoint. The *Maximum Resolution* settings for conferences and participants cannot be changed during an ongoing conference.
Video Clarity™	When enabled (default), *Video Clarity* applies video enhancing algorithms to incoming video streams of resolutions up to and including SD. Clearer images with sharper edges and higher contrast are sent back to all endpoints at the highest possible resolution supported by each endpoint. All layouts, including 1x1, are supported. **Note:** Video Clarity is enabled only when *Video Quality* is set to *Sharpness* (default setting) and is disabled when *Video Quality* is set to *Motion*. Video Clarity can only be enabled for Continuous Presence conferences in *MPM+* and *MPMx* Card Configuration Mode.
Auto Brightness	*Auto Brightness* detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout. • *Auto Brightness* is supported with MPM+ and MPMx cards only. • *Auto Brightness* only increases brightness and does not darken video windows. • *Auto Brightness* is selected by default. • *Auto Brightness* cannot be selected and deselected during an ongoing conference. **Default**: On **Note:** When *Auto Brightness* is enabled, color changes may be observed in computer-based *VGA Content* sent by *HDX* endpoints through the *People* video channel.

Table 2-11 *New AVC Profile - Video Quality Parameters (Continued)*

Field/Option	Description
Content Video Definition	
Content Settings	Select the transmission mode for the Content channel: • ***Graphics*** — basic mode, intended for normal graphics • ***Hi-res Graphics*** (AVC Only) — a higher bit rate intended for high resolution graphic display • ***Live Video*** (AVC Only) — Content channel displays live video • ***Customized Content Rate*** (AVC Only) **-** manual definition of the Conference Content Rate**,** mainly for cascading conferences. Selection of a higher bit rate for the *Content* results in a lower bit rate for the people channel. For a detailed description of each of these options, see "*Content Settings”* on page **4-7**.

Content Protocol	• **H.263** (AVC only)
	  • *Content* is shared using the *H.263* protocol.
	  • Use this option when most of the endpoints support *H.263* and some endpoints support *H.264*.
	• **H.263 & H.264 Auto Selection** (Default)
	  • *Content* is shared using *H.263* if a mix of H.263-supporting and *H.264*-supporting endpoints are connected.
	  • *Content* is shared using *H.264* if all connected endpoints have *H.264* capability.
	• **H.264 Cascade and SVC Optimized**
	  • All *Content* is shared using the *H.264* content protocol and is optimized for use in *Cascaded Conferences*.
	• **H.264 HD** (AVC only)
	  • Ensures high quality *Content* when most endpoints support *H.264* and *HD Resolutions*.
	For more information, see "*Content Protocols”* on page **4-8** and "*Defining Content Sharing Parameters for a Conference”* on page **4-13**.

10 Click the **Video Settings** tab.
The *New Profile - Video Settings* dialog box opens.



11 Define the video display mode and layout using the following parameters:

Table 2-12 *New AVC Profile - Video Settings Parameters*

Field/Option	Description
Presentation Mode (CP only)	Select this option to activate the Presentation Mode. In this mode, when the current speaker speaks for a predefined time (30 seconds), the conference changes to Lecture Mode. When another participant starts talking, the Presentation Mode is cancelled and the conference returns to the previous video layout.
Lecture View Switching	Select this option to enable automatic switching of participants on the Lecturer’s screen when Lecture Mode is enabled for the conference. The automatic switching is enabled when the number of participants exceeds the number of video windows displayed on the Lecturer’s screen. **Note:** Lecture Mode is enabled in the *Conference Properties – Participants* tab. For more information, see "*Lecture Mode (AVC Only)”* on page **4-73**.

Table 2-12 *New AVC Profile - Video Settings Parameters (Continued)*

Field/Option	Description

Send Content to Legacy Endpoints
 	
(CP only)
	When enabled (default), Content can be sent to H.323/SIP/ISDN endpoints that do not support H.239 Content (legacy endpoints) over the video (people) channel. For more information see Chapter 4, "*Sending Content to Legacy Endpoints (AVC Only)"* on page **4-17**.
	Notes:
	• This option is enabled in MPM+ and MPMx *Card Configuration Modes* only.
	• When enabled, additional video resources are allocated to the conference:
	  • In *MPM+* mode, an additional SD video resource is allocated.
	  • In *MPMx* mode, an additional HD video resource is allocated.
	• This option is valid when sending Content as a separate stream is enabled by the *System Flag* ENABLE_H239 set to YES.
	• Select this option when Avaya *IP Softphone* will be connecting to the conference.
	• If *High Definition Video Switching* option is selected in the *Conference Profile - General* tab, the *Send Content to Legacy Endpoints* selection is cleared and the option is disabled.
	• If the *Same Layout* option is selected, the *Send Content to Legacy Endpoints* selection is cleared and is disabled.
	• Once an endpoint is categorized as Legacy, it will not be able to restore its content to the Content channel and will receive content only in the video channel.
	• This option is automatically enabled when *H.264 Cascade Optimized* is selected as the *Content Protocol*. For more information see "*Content Protocols"* on page **4-8**.

Site Names **(MPM+ Only)** **(CP only)**	Clear this check box to hide the display of site names on the endpoint screens during the conference. When selected (default), *Site Names* are displayed during the conference, whenever the conference speaker changes. Prior to Version 7.6, *Site Names* display was enabled or disabled by the HIDE_SITE_NAMES *System Flag*. *Site Names* display is controlled by the following *System Flags*, as in previous versions: • SITE_NAME_TRANSPARENCY - Used to turn *Site Name Transparency* of 50% on or off. • SITE_NAMES_ALWAYS_ON - Enables the permanent display of *Site Names*. • SITE_NAMES_LOCATION - Changes the default location of the *Site Name* in the video layout.
Auto Scan Interval(s) **(CP only)**	Select the time interval, 10 - 300 seconds, that *Auto Scan* uses to cycle the display of participants that are not in the conference layout in the selected cell. *Auto Scan* is often used in conjunction with *Customized Polling* which allows the cyclic display to be set to a predefined order for a predefined time period.

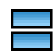
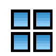
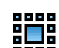
Table 2-12 New AVC Profile - Video Settings Parameters (Continued)

Field/Option	Description
Same Layout **(CP only)**	Select this option to force the selected layout on all participants in a conference. Displays the same video stream to all participants and personal selection of the video layout is disabled. In addition, if participants are forced to a video layout window, they can see themselves.
Auto Layout **(CP only)**	When selected (default), the system automatically selects the conference layout based on the number of participants currently connected to the conference. When a new video participant connects or disconnects, the conference layout automatically changes to reflect the new number of video participants. For more information, see Table 2-13 "*Auto Layout – Default Layouts"* on page **2-33**. Clear this selection to manually select a layout for the conference. The default Auto Layout settings can be customized by modifying default Auto Layout system flags in the System Configuration file. For more information see, "*Auto Layout Configuration"* on page **22-41**. **Note:** In some cases, the default layout automatically selected for the conference contains more cells than the number of connected participants, resulting in an empty cell. For example, if the number of connected participants is 4, the default layout is 2x2, but as only 3 participants are displayed in the layout (the participants do not see themselves), one cell is empty.
Telepresence Mode **(CP only)**	Select the *Telepresence Mode* from the drop-down menu: • **Off** - Normal conference video is sent by the RMX. • **Auto** (Default) - If any *ITP* (*Immersive Telepresence*) endpoints are detected, *ITP* features are applied to the conference video for all participants. When Auto is selected, the *ITP* features are dynamic. If all *ITP* endpoints disconnect from the conference, normal conference video is resumed for all participants. *ITP* features are resumed for all participants should an *ITP* endpoint re-connects to the conference. • **On** - ITP features are applied to the conference video for all participants regardless of whether there are *ITP* endpoints connected or not. **Notes:** • This field is enabled only if the RMX system is licensed for *Telepresence Mode*. • T*elepresence Mode* is unavailable in *Video Switching* conferences.

***Table 2-12** New AVC Profile - Video Settings Parameters (Continued)*

Field/Option	Description
Telepresence Layout Mode **(CP only)**	The *Telepresence Layout Mode* drop-down menu enables *VNOC* operators and *Polycom Multi Layout Applications* to retrieve *Telepresence Layout Mode* information from the RMX. The following modes can be selected: • Manual • Continuous presence - Room Continuous Presence (Default) • Room Switch - Voice Activated Room Switching **Note:** This field is enabled only if the RMXsystem is licensed for *Telepresence Mode*.

***Table 2-13** Auto Layout – Default Layouts*

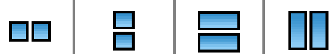
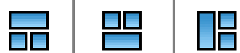
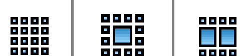
Number of Video Participants	Auto Layout Default Settings
0–2	
3	
4–5	
6–7	
8-10	
11	
12+	

In layout 2+8, the two central windows display the last two speakers in the conference: the current speaker and the “previous” speaker. To minimize the changes in the layout, when a new speaker is identified the “previous” speaker is replaced by the new speaker while the current speaker remains in his/her window.

> The RMX supports the VUI addition to the H.264 protocol for endpoints that transmit wide video (16:9) in standard 4SIF resolution.

12 To select the *Video Layout* for the conference, click the required number of windows from the layouts bar and then select the windows array. The selected layout is displayed in the *Video Layout* pane.

Table 2-14 *Video Layout Options*

Number of Video Windows	Available Video Layouts
1	
2	
3	
4	
5+	
9	
10+	
Overlay	 For more information see "*Overlay Layouts”* on page **2-61**.

When there is a change of speaker in a Continuous Presence conference, the transition is set by default to fade in the current speaker while fading out the previous speaker.

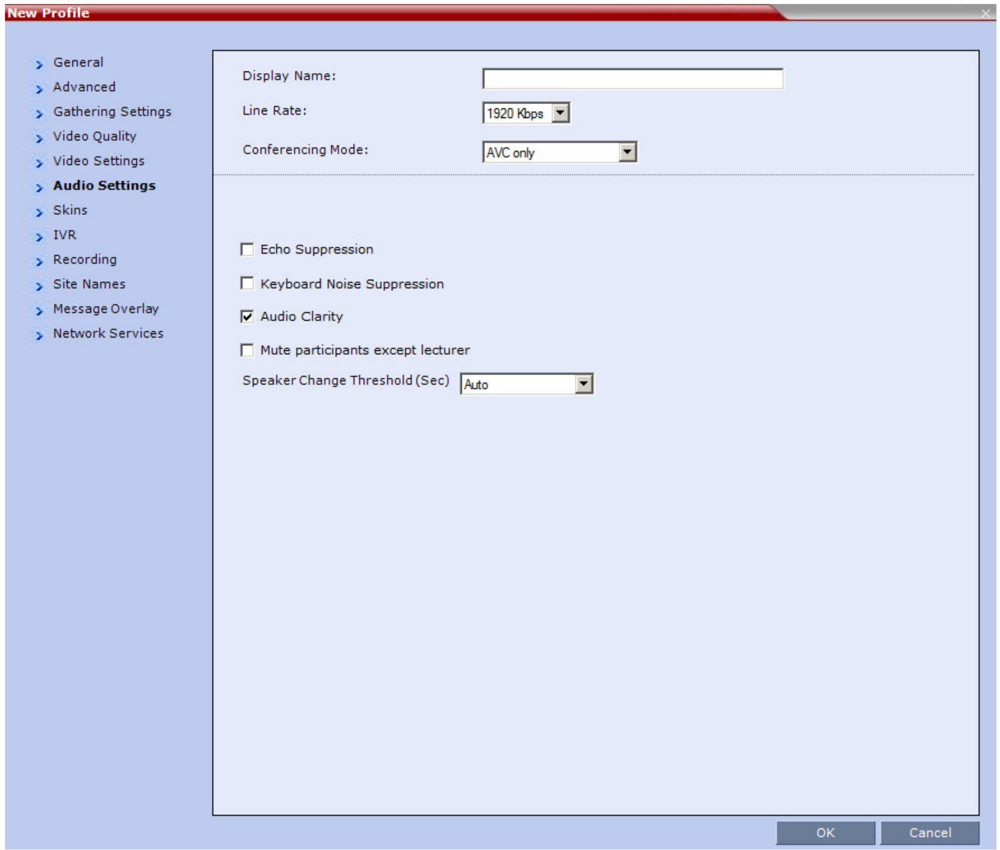
To make this transition visually pleasant, fading in the current speaker while fading out the previous speaker is done over a period of 500 milliseconds.

The *Fade In / Fade Out* feature can be disabled by adding a new flag to the *System Configuration*. The *Value* of the new flag must be: FADE_IN_FADE_OUT=NO.

Fade In / Fade Out is not supported with MPMx cards.

For more information about *System Flags*, see the *RealPresence Collaboration Server (RMX) 1500/ 2000/4000 Administrator’s Guide*, "*Modifying System Flags”* on page **22-1**.

13 Click the **Audio Settings** tab.
The *New Profile - Audio Settings* dialog box opens.



14 Define the video display mode and layout using the following parameters:

***Table 2-15** New AVC Profile - Audio Settings Parameters*

Field/Option	Description
Echo Suppression	When enabled (default), an algorithm is used to search for and detect echo outside the normal range of human speech (such as echo) and automatically mute them when detected. Clear this option to disable the Echo Suppression algorithm. **Notes:** • This option is activated only in *MPM+* and *MPMx Card Configuration Modes*. The CMA uses the *Profiles* that are stored in the RMX. When the *Echo Suppression* is enabled, it will be enabled in the conference that is started from the CMA with that *Profile*. However, the CMA does not display an indication that this option is enabled for the conference.

Table 2-15 *New AVC Profile - Audio Settings Parameters (Continued)*

Field/Option	Description
Keyboard Noise Suppression	Select this option to let the system use an algorithm to search for and detect keyboard noises and automatically mute them when detected. **Notes:** • This option is activated only in *MPM+* and *MPMx Card Configuration Modes*. • The CMA uses the *Profiles* that are stored in the RMX. When the *Keyboard Noise Suppression* is enabled, it will be enabled in the conference that is started from the CMA with that *Profile*. However, the CMA does not display an indication that this option is enabled for the conference.

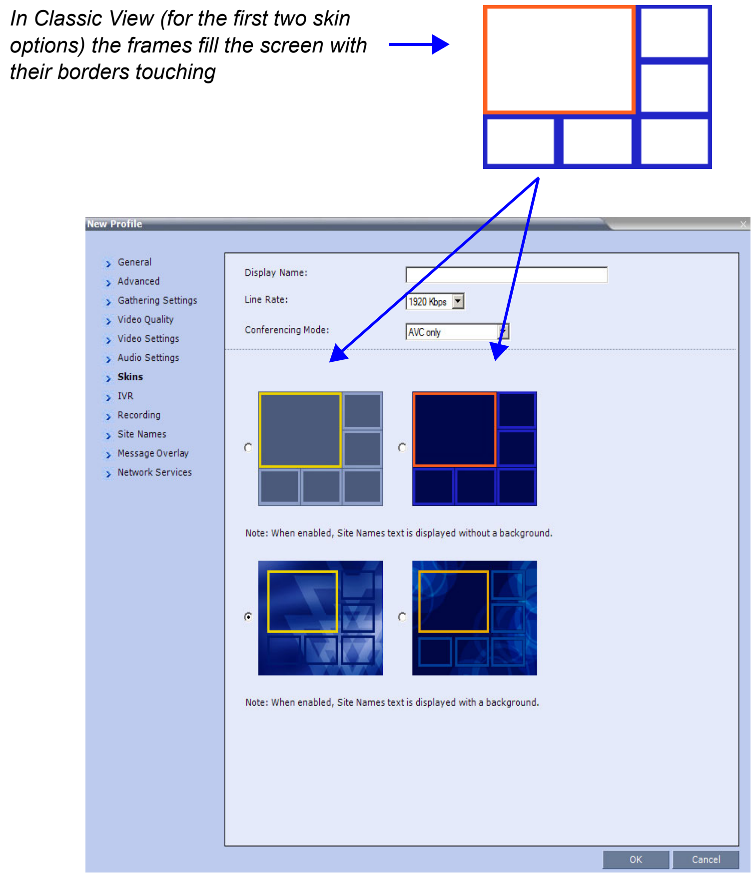
Audio Clarity	When selected, improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity.
	• The enhancement is applied to the following low bandwidth (8kHz) audio algorithms:
	  • G.729a
	  • G.711
	• Audio Clarity is supported with MPM+ and MPMx cards only.
	• Audio Clarity is selected by default.
	• Audio Clarity cannot be selected and deselected during an ongoing conference.

Speaker Change Threshold	Select the amount of time a participant must speak continuously before becoming the speaker. The possible values are: • Auto (Default, 3 seconds) • 1.5 seconds • 3 seconds • 5 seconds **Note:** This option can only be changed in *MPMx Card Configuration Mode*. in *MPM+ Card Configuration Mode* this value is always Auto.

***Table 2-15** New AVC Profile - Audio Settings Parameters (Continued)*

Field/Option	Description
Mute participant except lecturer	When the *Mute Participants Except Lecturer* option is enabled, the audio of all participants in the conference except for the lecturer can be automatically muted upon connection to the conference. This prevents other conference participants from accidentally interrupting the lecture, or from a noisy participant affecting the audio quality of the entire conference. Muted participants cannot unmute themselves unless they are unmuted from the RMX Web Client/RMX Manager. You can enable or disable this option during the ongoing conference. **Notes:** • When enabled, the mute indicator on the participant endpoints are not visible because the mute participants was initiated by the MCU. Therefore, it is recommended to inform the participants that their audio is muted by using the Closed Caption or Message Overlay functions. In the RMX Web Client/Manager, the mute by MCU indicator is listed for each muted participant in the *Audio* column in the *Participants* pane. • The *Mute Participants Except Lecturer* option can be disabled during an ongoing conference, thereby unmuting all the participants in the conference. • If the endpoint of the designated lecturer is muted when the lecturer connects to the conference, the lecturer remains muted until the endpoint has been unmuted. • When you replace a lecturer, the MCU automatically mutes the previous lecturer and unmutes the new lecturer. • When you disconnect a lecturer from the conference or the lecturer leaves the conference, all participants remain muted but are able to view participants in regular video layout until the you disable the *Mute Participants Except Lecturer* option. • A participant can override the *Mute Participants Except Lecturer* option by activating the *Mute All Except Me option* using the appropriate DTMF code, provided the participant has authorization for this operation in the *IVR Services*. The lecturer audio is muted and the participant audio is unmuted. You can reactivate the *Mute Participants Except Lecturer* option after a participant has previously activated the Mute All Except Me option. The participant is muted and the lecturer, if designated, is unmuted. • In cascaded conferences, all participants (including the link participants) are muted. Only the lecturer is not muted.

15 **For CP Conferences only:** Click the **Skins** tab to modify the background and frames. The *New Profile - Skins* dialog box opens.

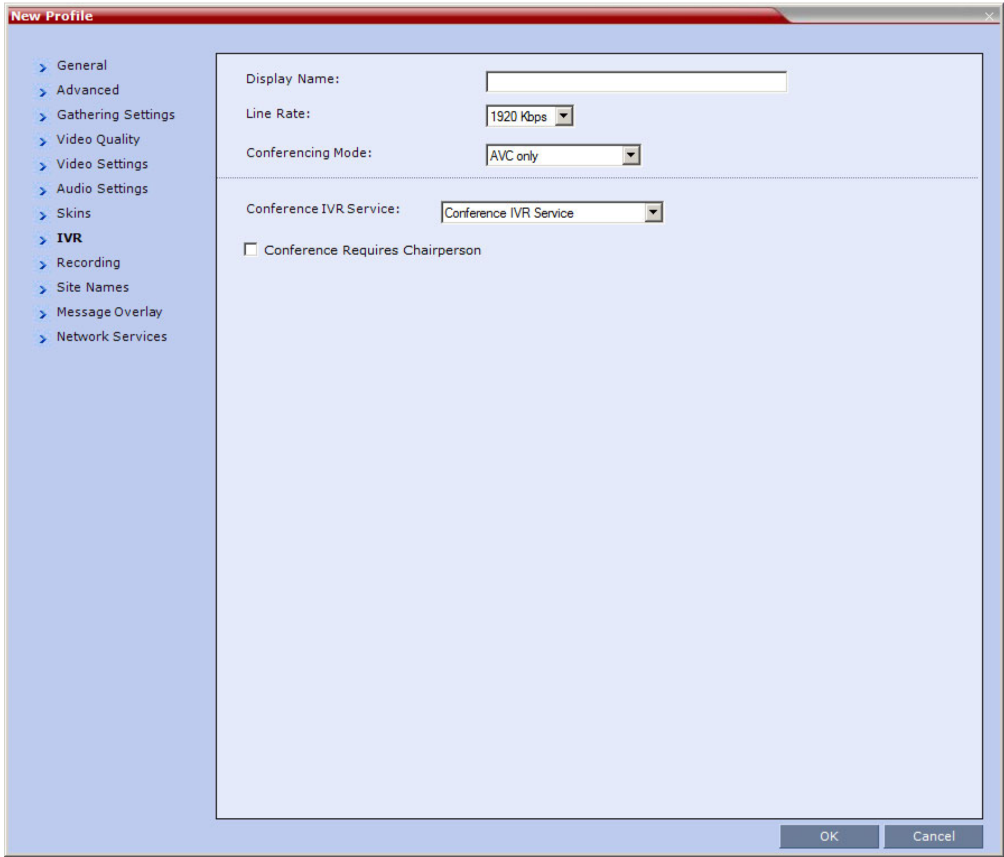


16 Select one of the *Skin* options.

When *Telepresence Mode* is enabled, the Skin options are disabled as the system uses a black background and the frames and speaker indication are disabled.

17 Click **IVR** tab.

The *New Profile - IVR* dialog box opens.



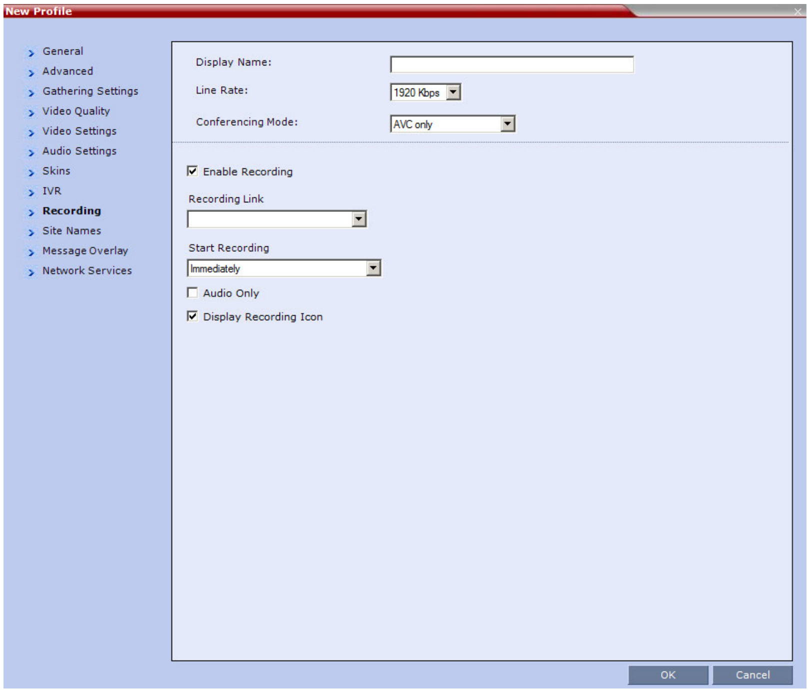
18 If required, set the following parameters:

Table 2-16 *New AVC Profile - IVR Parameters*

Field/Option	Description
Conference IVR Service	The default conference IVR Service is selected. You can select another conference IVR Service if required.
Conference Requires Chairperson	Select this option to allow the conference to start only when the chairperson connects to the conference and to automatically terminate the conference when the chairperson exits. Participants who connect to the conference before the chairperson are placed on *Hold* and hear background music (and see the *Welcome* video slide). Once the conference is activated, the participants are automatically connected to the conference. When the check box is cleared, the conference starts when the first participant connects to it and ends at the predefined time or according to the *Auto Terminate* rules when enabled. **Note**: This feature is implemented only if the *System Flag* TERMINATE_CONF_AFTER_CHAIR_DROPPED is set to YES.

19 **Optional**. Click the **Recording** tab to enable conference recording with *Polycom RSS 2000/4000*.

The *New Profile - Recording* tab opens.



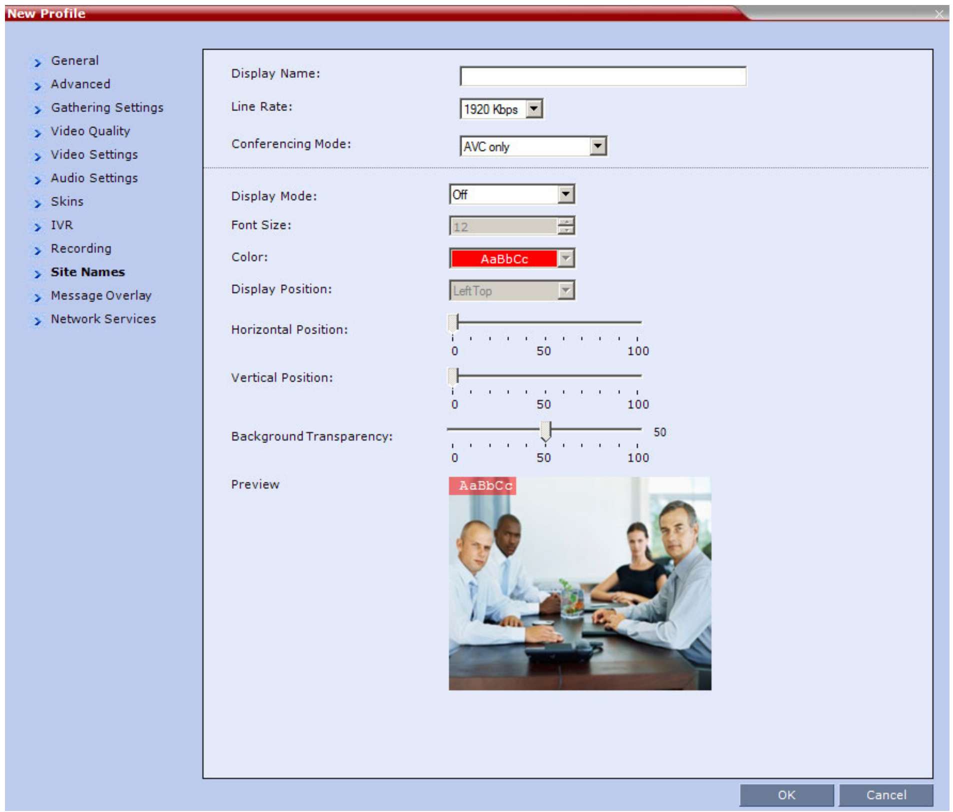
20 Define the following parameters:

Table 2-17 *New AVC Profile - Recording Parameters*

Parameter	Description
Enable Recording	Select this check box to enable the *Recording* settings. If no *Recording Links* are found an error message is displayed.
Recording Link	*Select the Recording Link to be used for conference recording.* *Recording Links* defined on the RMX can be given a descriptive name and can be associated with a *Virtual Recording Room (VRR)* saved on the *Polycom® RSS™ 4000 Version 6.0 Recording and Streaming Server* (*RSS*). For more information see "*Recording Conferences"* on page **14-1**.
Start Recording	Select one of the following: • **Immediately** – conference recording is automatically started upon connection of the first participant. • **Upon Request** – the operator or chairperson must initiate the recording (manual).
Audio Only	Select this option to record only the audio channel of the conference. **Note:** This option can be used only if there are Voice ports configured in the Video/Voice Port Configuration. For more information, see "*Video/Voice Port Configuration"* on page **21-10**.
Display Recording Icon	This option is automatically selected to display a *Recording Indication* to all conference participants informing them that the conference is being recorded.

The Recording participant does not support H.264 High Profile. If recording a conference set to H.264 High Profile, the Recording participant connects as Audio Only and records the conference Audio.

21 **For MPMx Card Configuration Mode and CP Conferences only:** Click the **Site Names** tab to display the *Site Names* dialog box.



Using the Site Name dialog box, you can control the display of the site names by defining the font, size, color, background color and transparency and position within the Video Window. For a detailed description of the site names options see "*Site Names Definition"* on page **2-64**.

22 Define the following parameters:

Table 2-18 *New AVC Profile - Site Names Parameters*

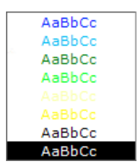
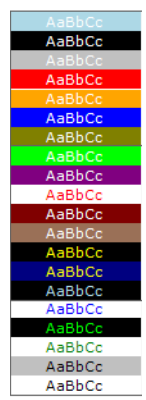
Field	Description
Display Mode	Select the display mode for the site names: • **Auto** - Display the *Site Names* for 10 seconds whenever the *Video Layout* changes. • **On** - Display the *Site Names* for the duration of the conference. • **Off** (default) - Do not display the *Site Names*. **Note:** The *Display Mode* field is grayed and disabled if *Video Switching* mode is selected in the *Profile - General* tab. If *Display Mode* is **Off**, all other fields in this tab are grayed and disabled. Selecting **Off** enables *Video Switching* for selection in the *Profile - General* tab (if the conference is not already ongoing).
Font Size	Click the arrows to adjust the font size (in points) for the *Site Names* display. **Range:** 9 - 32 points **Default:** 12 **Note:** Choose a *Font Size* that is suitable for viewing at the conference’s video resolution. For example, if the resolution is *CIF*, a larger *Font Size* should be selected for easier viewing.
Background Color	Select the color of the *Site Names* display text. The color and background for *Site Names* display text is dependent on whether a *Plain Skin* or a *Picture Skin* was selected for the conference in the *Profile - Skins* tab. The choices are: **Plain Skin**  **Default:** White Text No Background (For contrast, no background is shown as black when the text is white.) **Picture Skin**  **Default:** White Text Red Background **Note:** Choose a *Background Color* combination that is suitable for viewing at the conference’s video resolution. At low resolutions, it is recommended to select brighter colors as dark colors may not provide for optimal viewing.

Table 2-18 *New AVC Profile - Site Names Parameters (Continued)*

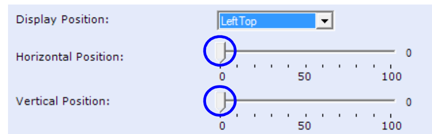
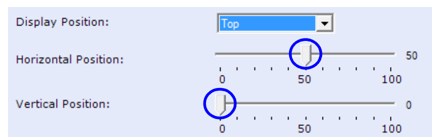
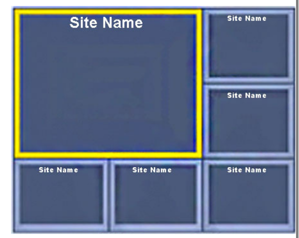
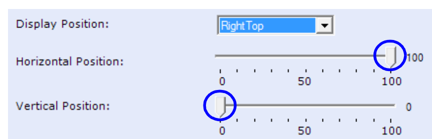
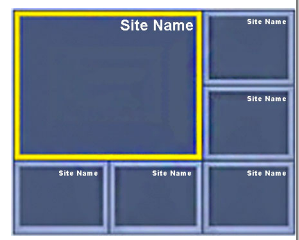
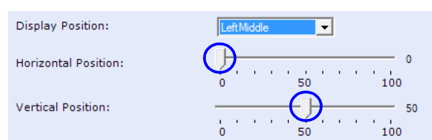
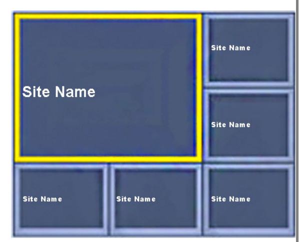
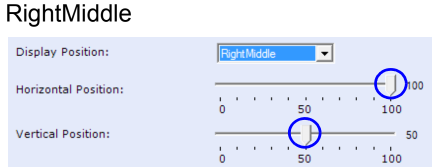
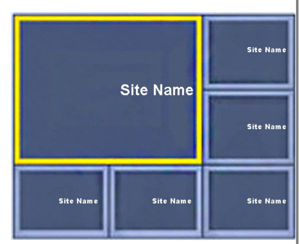
Field	Description
Display Position	Select the pre-set position for the display of the *Site Names.* ***Selection*** — ***Site Names Position*** LeftTop (Default)   Top   RightTop   LeftMiddle   RightMiddle  

Table 2-18 *New AVC Profile - Site Names Parameters (Continued)*

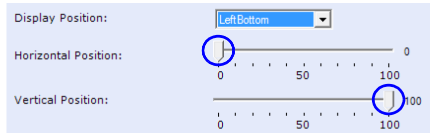
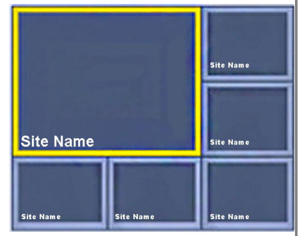
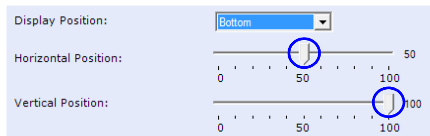
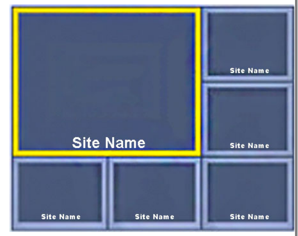
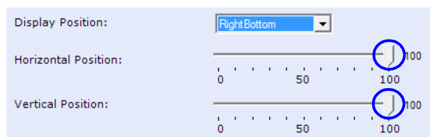
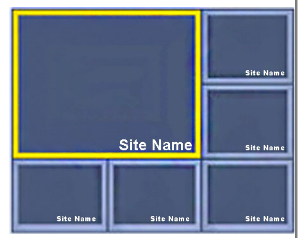
<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td rowspan="4">Display Position (cont.)</td><td>LeftBottom
</td><td></td></tr>
<tr><td>Bottom
</td><td></td></tr>
<tr><td>RightBottom
</td><td></td></tr>
<tr><td>Custom</td><td>The current Site Names display position becomes the initial position for Site Names position adjustments using the Horizontal and Vertical Position sliders.</td></tr>
<tr><td>Horizontal Position</td><td>Move the slider to the left to move the horizontal position of the Site Names to the left within the Video Windows.
Move the slider to the right to adjust the horizontal position of the Site Names to the right within the Video Windows.</td><td rowspan="2">Note: Use of these sliders will set the Display Position selection to Custom.</td></tr>
<tr><td>Vertical Position</td><td>Move the slider to the left to move the vertical position of the Site Names upward within the Video Windows.
Move the slider to the right to move the vertical position of the Site Names downward within the Video Windows.</td></tr>
</table>

Table 2-18 *New AVC Profile - Site Names Parameters (Continued)*

Field	Description
Background Transparency	Move the slider to the left to decrease the transparency of the background of the *Site Names* text. 0 = No transparency (solid background color). Move the slider to the right to increase the transparency of the background of the *Site Names* text. 100 = Full transparency (no background color) **Default:** 50 **Note:** This slider is only displayed if a *Picture Skin* is selected.

23 **For CP Conferences only:** Click the **Message Overlay** tab to display the *Message Overlay* dialog box.

Message Overlay in **MPM+** Card Configuration Mode

Message Overlay in **MPMx** Card Configuration Mode

Message Overlay enables you to send text messages to all participants during ongoing Continuous Presence conferences.

The text message is seen as part of the in the participant's video layout on the endpoint screen or desktop display.

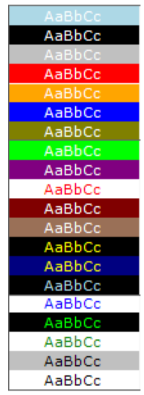
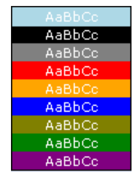
For more details, see "*Message Overlay for Text Messaging"* on page **2-67**.

Define the following fields:

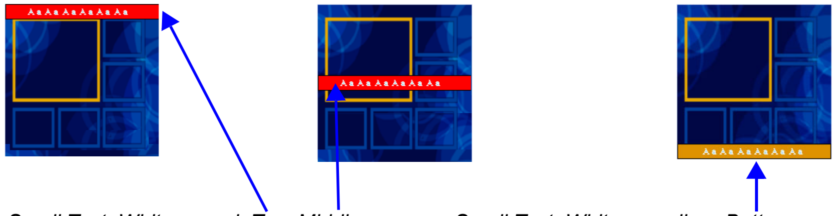
Table 2-19 *New AVC Profile - Message Overlay Parameters*

Field	Description
Enable	Select this check box to enable *Message Overlay*. Clear this check box to disable *Message Overlay*. **Default:** Cleared. **Note:** • The *Message Overlay* field is shaded and disabled when *Video Switching* mode is selected in the *New Profile - General* tab. All other fields in this tab are also disabled. • Clearing the *Enable* check box enables *Video Switching* for selection in the *New Profile - General* tab. • If *Message Overlay* is selected, the *Video Switching* check box in the *New Profile - General* tab is disabled and cannot be selected.
Content	Enter the message text. The message text can be up to 50 (MPMx) or 32 (MPM+) Chinese characters.
Font Size	**In MPMx Card Configuration Mode:** Click the arrows to adjust the font size (points) for the *Message Overlay* display. **Range:** 9 - 32 **Default:** 24 **In MPM+ Card Configuration Mode:** Select the size of the text font from the list: Small, Medium or Large. **Default:** Small **Note:** In some languages, for example Russian, when a large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.

Table 2-19 New AVC Profile - Message Overlay Parameters (Continued)

Field	Description
Color	From the drop-down menu select the color and background of the *Message Overlay* display text. The choices are:  **MPMx Mode** Color Options  **MPM+ Mode** Color Options **Default:** White Text on Red Background.
Vertical Position (**MPMx** Card Configuration Mode Only)	Move the slider to the **right** to move the vertical position of the *Message Overlay* **downward** within the *Video Layout.* Move the slider to the **left** to move the vertical position of the *Message Overlay* **upward** within the *Video Layout.* **Default:** Top Left (10)
Background Transparency (**MPMx** Card Configuration Mode Only)	Move the slider to the **left** to **decrease** the transparency of the background of the *Message Overlay* text. 0 = No transparency (solid background color). Move the slider to the **right** to **increase** the transparency of the background of the *Message Overlay* text. 100 = Full transparency (no background color). **Default:** 50
Display Repetition	Click the arrows to increase or decrease the number of times that the text message display is to be repeated. **Default:** 3
Display Position (**MPM+** Card Configuration Mode Only)	Select the position for the display of the Message Overlay on the endpoint screen: • Top • Middle • Bottom **Default:** Bottom
Display Speed	Select whether the text message display is static or moving across the screen, the speed in which the text message moves: • Static • Slow • Fast **Default:** Slow

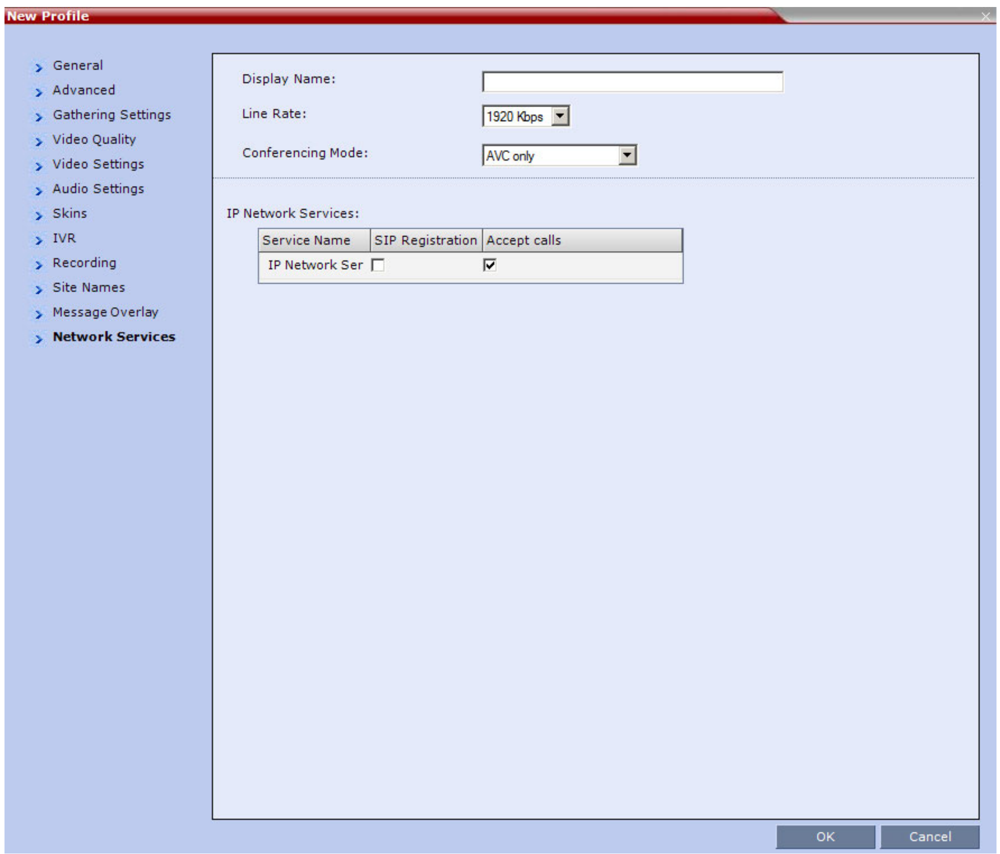
As the fields are modified the *Preview* changes to show the effect of the changes.
For example:



Small Text, White on red, Top, Middle *Small Text, White on yellow, Bottom*

24 Click the **Network Services** tab.

The *New Profile - Network Services* tab opens.



Registration of conferencing entities such as ongoing conferences, Meeting Rooms, Entry Queues, SIP Factories and Gateway Sessions with SIP servers is done per conferencing entity. This allows better control on the number of entities that register with each SIP server. Selective registration is enabled by assigning a conference Profile in which registration is configured to the required conferencing entities. Assigning a conference Profile in which registration is not configure to conferencing entities will prevent them from registering. By default, Registration is disabled in the Conference Profile, and must be enabled in Profiles assigned to conferencing entities that require registration.

25 Define the following parameters:

Table 2-20 *New AVC Profile - Network Services Parameters*

Parameter	Description
IP Network Services:	
Service Name	This column lists all the defined *Network Services,* one or several depending on the system configuration.
SIP Registration	To register the conferencing entity to which this profile is assigned with the SIP Server of the selected *Network Service*, click the check box of that *Network Service* in this column. When SIP registration is not enabled in the conference profile, the RMX's registering to SIP Servers will each register with an URL derived from its own signaling address. This unique URL replaces the non-unique URL, dummy_tester, used in previous versions.
Accept Calls	To prevent dial in participants from connecting to a conferencing entity when connecting via a *Network Service*, clear the check box of the *Network Service* from which calls cannot connect to the conference.

26 Click **OK** to complete the *Profile* definition.
A new *Profile* is created and added to the *Conference Profiles* list.

Defining a Video Switching Conference Profile

A Video Switching-enabled Profile must be created prior to running Video Switching conferences.

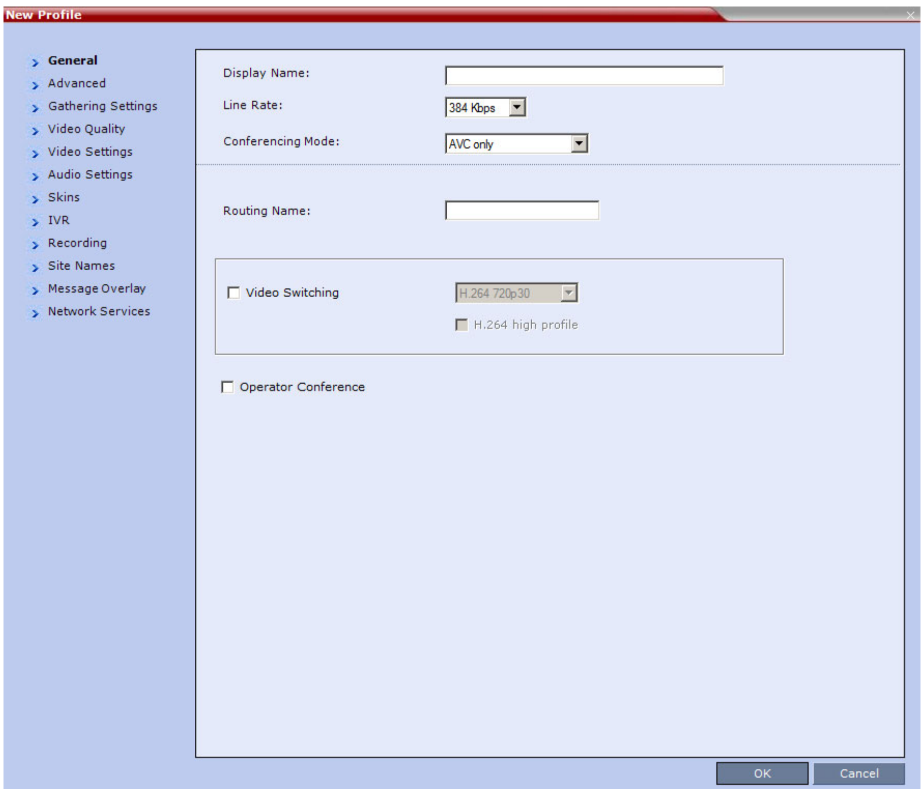
Video Switching conferences and Meeting Rooms are created by selecting a Video Switching-enabled Profile and must be set to the same line rate as the target conference.

To connect to an Video Switching conference via an Entry Queue, the Entry Queue must be Video Switching enabled. It is recommended to use the same Profile for both the target conference and Entry Queue.

To Create a Video Switching-enabled Profile:

1 In the *RMX Management* pane, click **Conference Profiles**.

2 In the *Conference Profiles* pane, click the **New Profile** button.
The *New Profile – General* dialog box opens.



3 Define the *Profile* name and, if required, the *Profile - General* parameters:

Table 2-21 *New AVC Profile (VSW) - General Parameters*

Field/Option	Description
Display Name	Enter a unique Profile name, as follows: • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. It is recommended to use a name that indicates the Profile type, such as Operator conference or Video Switching conference. **Note:** This field is displayed in all tabs.
Line Rate	Select the conference bit rate. The line rate represents the combined video, audio and Content rate. When defining a VSW profile, select a line rate that all connecting participants can use. Participants that their endpoint or network that do not support this line rate cannot connect to the conference or will connect as Audio Only (if resources were designated as Voice ports). If a high definition resolution will be selected for the conference video, make sure that the selected line rate is higher than the line rate minimum threshold defined in the flag HD_THRESHOLD_BITRATE for HD video Switching conferences. The default setting is 384 Kbps. **Notes:** • This field is displayed in all tabs. • Maximum line rate at which ISDN endpoints can connect to a conference is 768 kbps.
Conferencing Mode	Make sure that **AVC Only** is selected (default) to define a VSW conference Profile. **Note:** This field is displayed in all tabs.
Routing Name	Enter the *Profile* name using ASCII characters set. The Routing Name can be defined by the user or automatically generated by the system if no Routing Name is entered as follows: • If an all ASCII text is entered in Display Name, it is used also as the Routing Name. • If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name.

Table 2-21 *New AVC Profile (VSW) - General Parameters (Continued)*

Field/Option	Description
Video Switching	If the *Operator Conference* option is selected, this option is disabled, and the selection is cleared. • Select this check box to create a Video Switching profile. • Then select the video protocol and resolution for the conference. Resolution supported by MPM media cards: • H.264 720p30 Resolutions supported by MPM+ and MPMx cards only: • H.264 1080p60 • H.264 1080p30 • H.264 720p60 • H.264 720p30 • H.264 SD 30 • H.264 CIF • H.263 CIF • H.261 CIF When selected, the conference is in a special conferencing mode which implies that all participants must connect at the same line rate and use the same video resolution. Participants with endpoints that do not support the selected line rate and resolution will connect as secondary (audio only). For more information, see "*Video Switching (VSW) Conferencing"* on page **2-4**. **Notes:** • Video Switching conferencing mode is unavailable to ISDN participants. • To connect to a Video Switching conference via Entry Queue, the Profile assigned to the Entry Queue must be set to Video Switching. It is recommended to use the same profile for both the destination conference and Entry Queue. • *Telepresence Mode* is unavailable in *Video Switching* conferences.
H.264 High Profile	Select this check box to enable the use of *H.264 High Profile* in *Video Switching* conferences. The *High Profile* check box is only displayed if MPMx cards are installed in the RMX. By default the High Profile check box is not selected. If H.264 is not the selected video protocol the check box is inactive (grayed out). For more information, see *"H.264 High Profile Support in Video Switching Conferences"* on page **2-53**.

Table 2-21 *New AVC Profile (VSW) - General Parameters (Continued)*

Field/Option	Description
Operator Conference ***(CP Only)***	Select this option to define the profile of an Operator conference. An Operator conference can only be a Continuous Presence conference, therefore when selected, the *Video Switching* option is disabled and cleared. When defining an *Operator Conference*, the *Send Content to Legacy Endpoints* option in the *Video Settings* tab is cleared and disabled. For more information, see Chapter 10, "*Operator Assistance & Participant Move"* on page **10-1**.

Selecting a new conference line rate lower than the initial line rate selected for the conference (for example, changing from 4096 kbps to 1532 kbps) may result in system reverting to the default resolution for that line rate (for example, 720p instead of 1080p). You may need to select the required resolution again, provided the selected line rate is higher than the minimum threshold line rate defined for that resolution in the system configuration. For more details, see "Minimum Threshold Line Rate System Flags" below.

When *Video Switching* is selected for the conference, the following options are **not available**:

— Operator Conference

— Gathering Phase

— Video Settings:

- Presentation Mode
- Send Content To Legacy Endpoints
- Auto Layout/Same Layout (only full screen, 1x1 layout display is available)
- Auto Scan

— Skins

— Site Names

— Message Overlay

4 Define the various Profile parameters. For more information, see "*Defining AVC Conferencing Profiles"* on page **2-19**.

5 Click **OK**.

H.264 High Profile Support in Video Switching Conferences

Beginning with *Version 7.6*, the *H.264 High Profile* video protocol is supported in *Video Switching* (*VSW*) conferences.

Guidelines

- **H.264 High Profile is supported in VSW conferences:**

  — With *MPMx* cards.

  — In *H.323* and *SIP* networking environments only (*VSW* conferences are not supported in *ISDN* networking environments.)

- **For H.264 High Profile-enabled VSW conferences:**

  — All endpoints connecting to the conference must support *High Profile*.

  — *High Profile-enabled* endpoints must connect to the VSW conference at the exact *line rate* and exact *resolution* defined for the conference.

— Endpoints that do not support *High Profile,* connecting to the VSW conference at the exact *line rate* and exact *resolution* defined for the conference are connected to the conference as *Secondary* (audio only).

- **For H.264 Base Profile VSW conferences:**

— *High Profile* supporting and non-*High Profile* supporting endpoints connect to the VSW conference using the *H.264 Base Profile* video protocol.

— Endpoints that do not support the exact conference *line rate* are disconnected.

— Endpoints that do not support the exact video settings such as protocol and *resolution* defined for the conference will be connected as *Secondary* (audio only).

Minimum Threshold Line Rate System Flags

The following table lists the *System Flags* that control the *minimum threshold line rate* for the various *resolutions* available for *High Profile*-enabled *VSW* conferences.

Table 2-22 *System Flags - Minimum Threshold Line Rates*

Flag Name	Minimum Threshold Line Rate (Kbps)
*VSW_**CIF**_HP_THRESHOLD_BITRATE*	64
*VSW_**SD**_HP_THRESHOLD_BITRATE*	128
*VSW_**HD720p30**_HP_THRESHOLD_BITRATE*	512
*VSW_**HD720p50-60**_HP_THRESHOLD_BITRATE*	832
*VSW_**HD1080p**_HP_THRESHOLD_BITRATE*	1024
*VSW_**HD1080p60**_HP_THRESHOLD_BITRATE*	1024
*VSW_**HD_1080p60**_BL_THRESHOLD_BITRATE*	1728

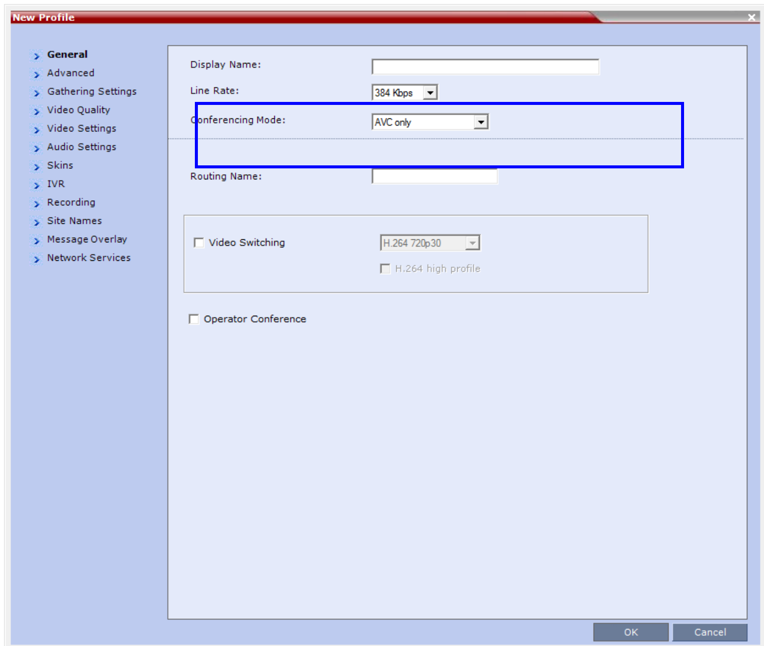
- *Line rate* and *resolution* combinations are checked for validity. If the selected *line rate* is below the *minimum threshold line rate* required for the selected *resolution*, the *line rate* is automatically adjusted to the *minimum threshold line rate* value for the selected *resolution.*
- The value of the **SUPPORT_HIGH_PROFILE** *System Flag* (used for *CP* conferences) has no effect on *VSW* conferences.
- Before they can be modified, all of the *System Flags* mentioned above must be added to the *system.cfg* file using the *RMX Menu – Setup* option. For more information see "*Modifying System Flags”* on page **22-1**.

Defining SVC Conferencing Profiles

To define SVC Only Profile:

1 In the *RMX Management* pane, click **Conference Profiles**.

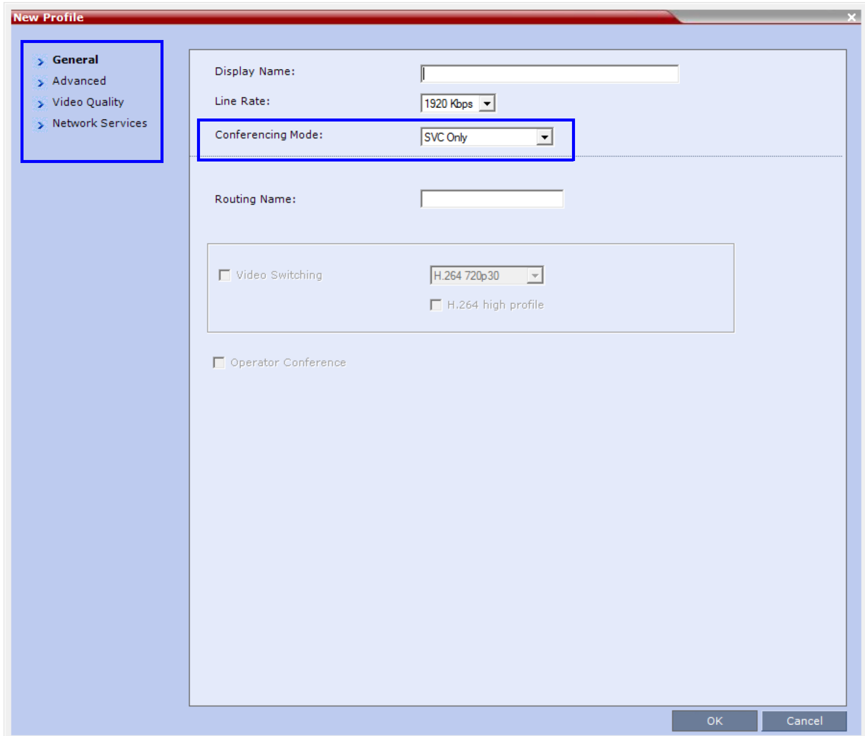
2 In the *Conference Profiles* pane, click the **New Profile** button.
The *New Profile – General* dialog box opens.



By default, the Profile is set to *AVC Only Conferencing Mode*.

3 In the *Conferencing Mode* list, select **SVC Only** to define an SVC Profile.

The profile tabs and options change accordingly and only supported options are available for selection. Unsupported options are disabled (grayed out).



4 Define the *Profile* name and, if required, the *Profile - General* parameters:

Table 2-23 *New SVC Profile - General Parameters*

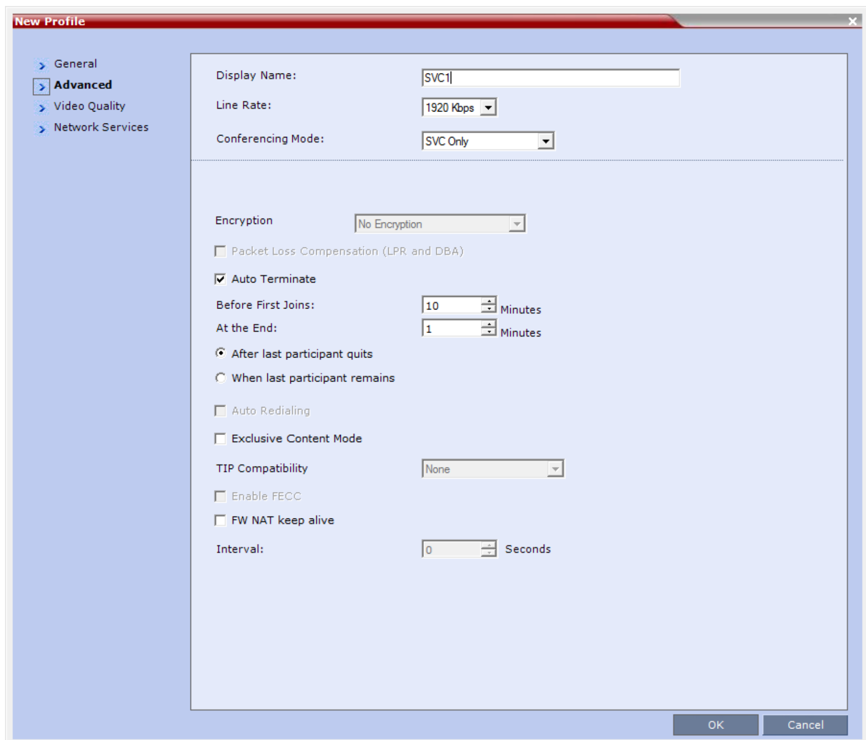
Field/Option	Description
Display Name	Enter a unique Profile name, as follows: • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. It is recommended to use a name that indicates the Profile type, such as Operator conference or Video Switching conference. **Note:** This is the only parameter that must be defined when creating a new profile. **Note:** This field is displayed in all tabs.
Line Rate	Select the conference bit rate. The line rate represents the combined video, audio and Content rate. The default setting for SVC Only conference is 1920kbps. **Notes:** • This field is displayed in all tabs.

Table 2-23 *New SVC Profile - General Parameters (Continued)*

Field/Option	Description
Routing Name	Enter the *Profile* name using ASCII characters set. The Routing Name can be defined by the user or automatically generated by the system if no Routing Name is entered as follows: • If an all ASCII text is entered in Display Name, it is used also as the Routing Name. • If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name.

5 Click the **Advanced** tab.

The *New Profile – Advanced* dialog box opens.



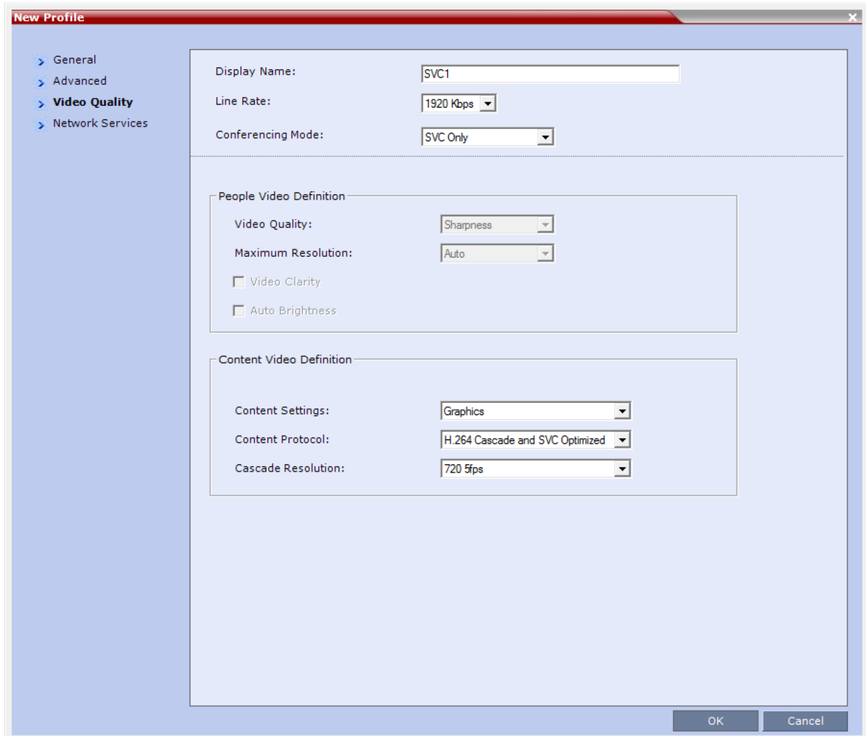
6 Define the following supported parameters:

Table 2-24 *New SVC Profile - Advanced Parameters*

Field/Option	Description
Auto Terminate	When selected (default), the conference automatically ends when the termination conditions are met: ***Before First Joins*** — No participant has connected to a conference during the *n* minutes after it started. Default idle time is 10 minutes. ***At the End - After Last participant Quits*** — All the participants have disconnected from the conference and the conference is idle (empty) for the predefined time period. Default idle time is 1 minute. ***At the End - When Last Participant Remains*** — Only one participant is still connected to the conference for the predefined time period (excluding the recording link which is not considered a participant when this option is selected). It is not recommended to select this option for SVC Conferences. Default idle time is 1 minute.
Exclusive Content Mode	When selected, *Content* broadcasting is limited to one participant preventing other participants from interrupting the Content broadcasting while it is active. For more details, see
FW NAT Keep Alive	When selected, an *FW NAT Keep Alive* message is sent at an interval defined in the field below the check box.
Interval	The time in seconds between *FW NAT Keep Alive* messages.

7 Click the **Video Quality** tab.

The *New Profile – Video Quality* dialog box opens.



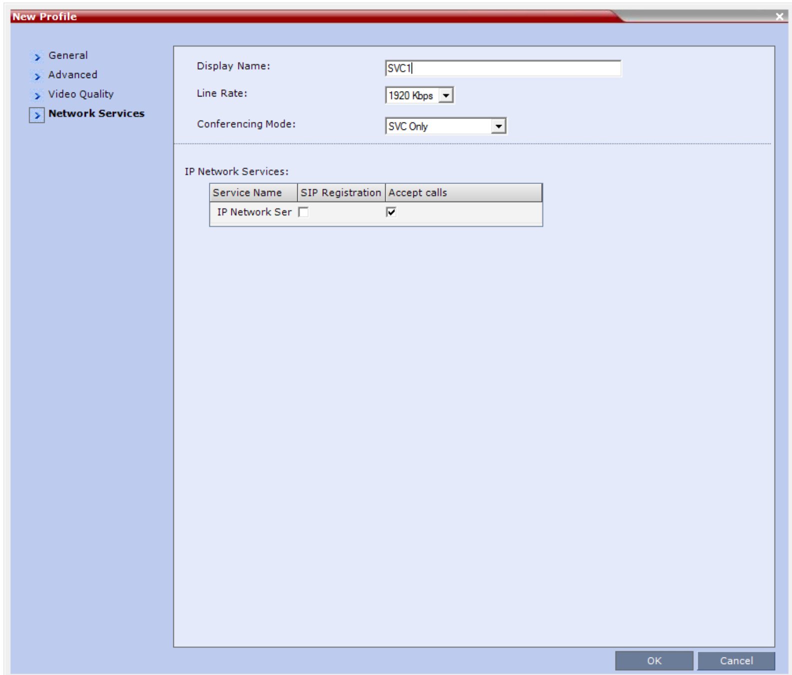
8 Define the following parameters:

Table 2-25 *New SVC Profile - Video Quality Parameters*

Field/Option	Description
Content Video Definition	
Content Settings	Only **Graphics** is available in SVC Conferencing Mode for transmission of Content. It offers the basic mode, intended for normal graphics For more information, see "*H.239"* on page **4-2**.
Content Protocol	**H.264 Cascade and SVC Optimized** is the only available Content Protocol for content sharing during SVC-based conferences. In this mode, all *Content* is shared using the *H.264* content protocol and all endpoints must use the set video resolution and frame rate (720p 5fps). Endpoints that do not support these settings cannot share content.

9 Click the **Network Services** tab.

The *New Profile - Network Services* tab opens.



Registration of conferencing entities such as ongoing conferences, Meeting Rooms, and SIP Factories with SIP servers is done per conferencing entity. This allows better control of the number of entities that register with each SIP server. Selective registration is enabled by assigning a conference Profile in which registration is configured for the required conferencing entities. Assigning a conference Profile in which registration is not configure for conferencing entities will prevent them from registering. By default, Registration is disabled in the Conference Profile, and must be enabled in Profiles assigned to conferencing entities that require registration.

10 Define the following parameters:

Table 2-26 *New SVC Profile - Network Services Parameters*

Parameter	Description
IP Network Services:	
Service Name	This column lists all the defined *Network Services*, one or several depending on the system configuration.
SIP Registration	To register the conferencing entity to which this profile is assigned with the SIP Server of the selected *Network Service*, click the check box of that *Network Service* in this column. When SIP registration is not enabled in the conference profile, the RMX's registering to SIP Servers will each register with an URL derived from its own signaling address. This unique URL replaces the non-unique URL, dummy_tester, used in previous versions.

***Table 2-26** New SVC Profile - Network Services Parameters (Continued)*

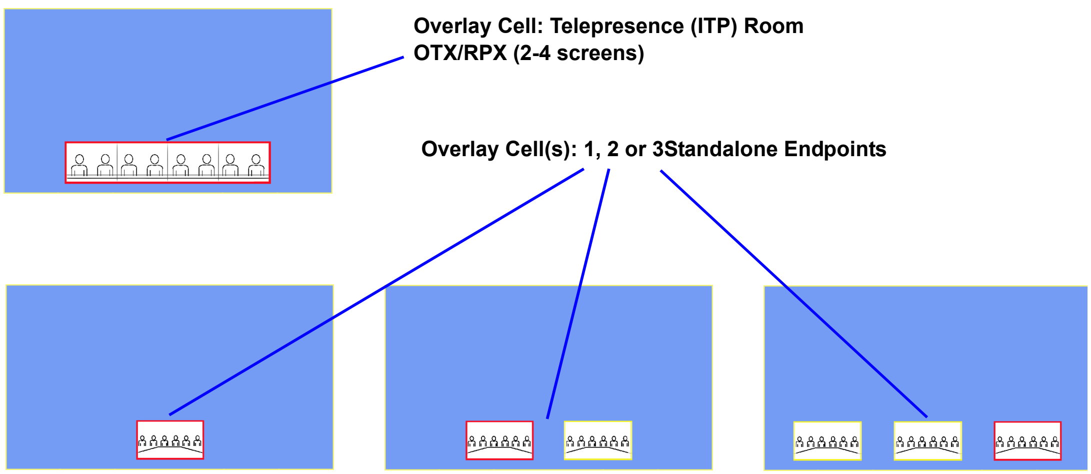
Parameter	Description
Accept Calls	To prevent dial in participants from connecting to a conferencing entity when connecting via a *Network Service*, clear the check box of the *Network Service* from which calls cannot connect to the conference.

11 Click **OK** to complete the *Profile* definition.
A new *Profile* is created and added to the *Conference Profiles* list.

CP Conferencing Additional Information

Overlay Layouts

Overlay Layouts allow additional participant endpoints to be displayed in 1x1 conference *Video Layout*s. The following *Overlay Layouts* are available:



Guidelines

- The *Overlay Layouts* are supported:
  - — With *MPMx* cards only.
  - — In RMX *CP* mode only.
  - — With *ITP*, non-*ITP* and *CTS* endpoints. Support of *ITP* and *CTS* requires *MLA* as a system component. (For more information see the *Polycom® Multipoint Layout Application (MLA) User's Guide for Use with Polycom Telepresence Solutions).*
  - — With both new and old *Skins* in RMX *CP* mode. *Skins* do not apply to *ITP* conferences.
- The *Overlay Layouts* are 20% of the height of the endpoint display and are supported on endpoints of both 16:9 and 4:3 aspect ratios.
- *Overlay Layouts* are recommended for use with high resolution endpoints.

- *Overlay Layouts* are not selected as defaults by the system. Default layouts are selected as in previous versions and are described in detail in "*Auto Layout – Default Layouts*" on page **2-33**.
- The *Overlay Layouts* are not available for selection when using *PCM* or *Click&View* for *Personal Layout* selection. *PCM* menus are not affected by the use of *Overlay Layouts* and are displayed as the top level overlay.
- *Message Overlay* is not affected by the use of *Overlay Layouts* and is displayed as the top level overlay.
- *Vertical Position* for *Site Name* display: *Site Names* are displayed for all cells. Because the smaller cells are located at the bottom of the large cell, when enabling *Site Names* it is advisable not to locate the *Site Name* at the bottom of the cells.

Telepresence (ITP) Room Layout Overlay

- The *Telepresence (ITP) Room Layout Overlay* is displayed with a border of the selected *Skin's* border color for the entire room while no border is displayed between the individual room cameras. For more information see "*Skins*" on page **2-38**.
- When an *ITP Room* is selected for as an overlay cell, only *Telepresence Room* names are listed for selection in the drop-down menu - not the individual endpoints in the *ITP Room*.
  If **Auto** is selected in the drop-down menu, the overlay cell will display the active speaker unless the active speaker is the large cell. If the endpoint itself is the current speaker, the previous speaker is displayed.

  For more information see "*Selecting the Overlay Layouts*" on page **2-63**. All other System behavior for *Video Forcing* and *Personal Layout Control* using the *Overlay Layouts* during an ongoing conference is the same as for previous versions and is described in the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide:*

  — "*Video Forcing (AVC-based Conferences)*" on page **3-58**

  — "*Personal Layout Control with the RMX Web Client*" on page **3-68**.

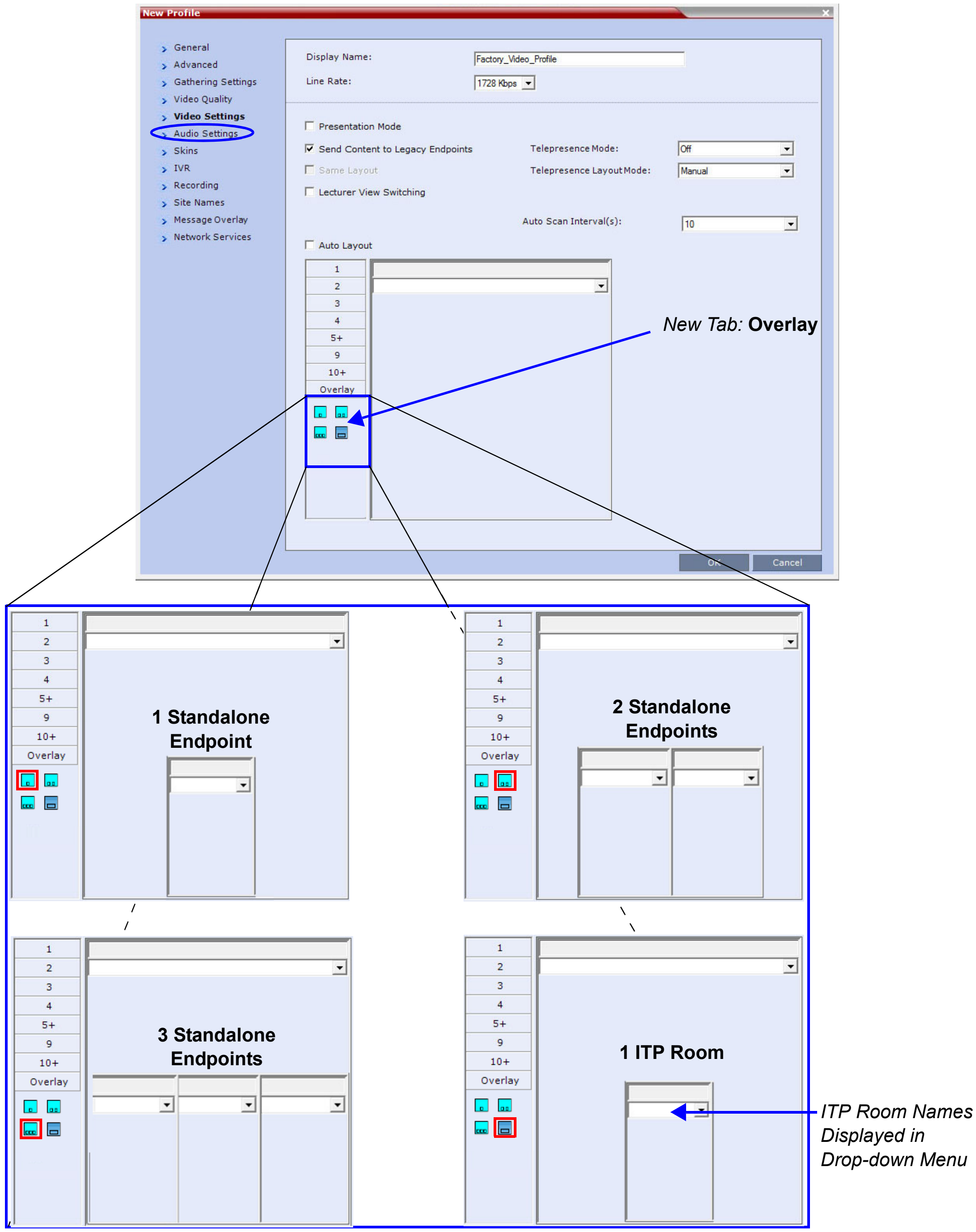
Standalone Endpoint Layout Overlay

- Each *Standalone Endpoint Layout Overlay* is displayed with a border of the selected *Skin's* border color. For more information see "*Skins*" on page **2-38**.

Selecting the Overlay Layouts

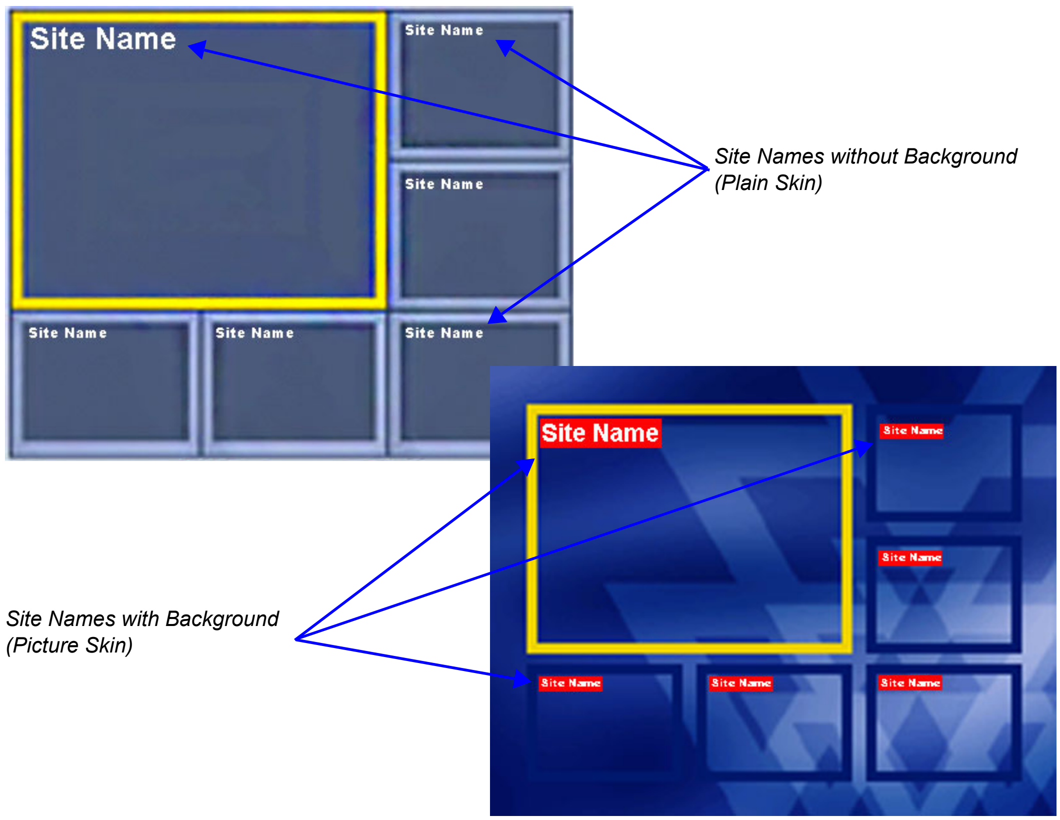
The *Overlay Layouts* are selected using the *New Profile - Video Settings* dialog box.

An additional tab, **Overlay**, has been added and includes the additional layout options.



Site Names Definition

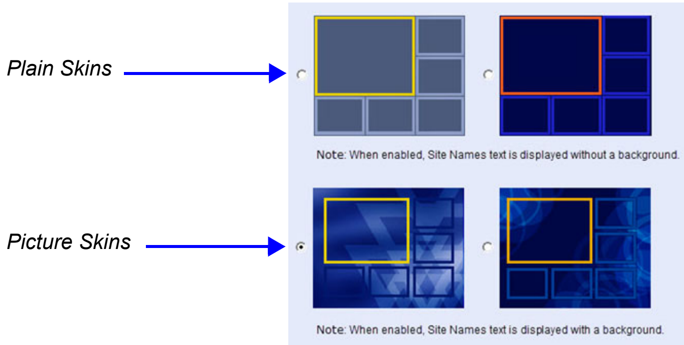
Using the *Site Name* dialog box, you can control the display of the site names by defining the font, size, color, background color and transparency and position within the *Video Window*.



Guidelines

- Only *MPMx* cards are supported.
- *Site Names* display is **Off** by default in a new profile.
- *Site Names* can be enabled to function in one of two modes:
  - **Auto** – Site names are displayed for 10 seconds whenever the conference layout changes.
  - **On** – Site names are displayed for the duration of the conference.
- During the display of the site names, the video frame rate is slightly reduced
- *Site Names* display is not available for *Video Switching* (*VSW*) conferences.
- *Site Names* display characteristics (position, size, color) can by modified during an ongoing conference using the *Conference Properties - Site Names* dialog box. Changes are immediately visible to all participants.
- *Site Names* display text and background color is dependent on the *Skin* selected for the conference:
  - **Plain Skins** - *Site Names* text is displayed without a background.

— **Picture Skins** - *Site Names* text is displayed with a background.



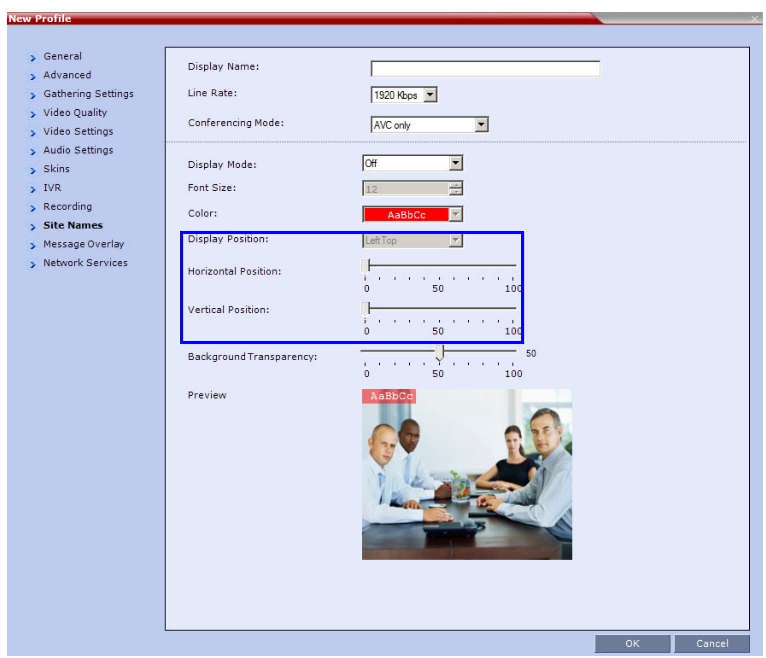
- In *MPMx Card Configuration Mode,* the *Site Names* tab options replace the functionality of the *System Flags* that were used in versions 7.6 and earlier (as for MPM+).
- In *MPM+ Card Configuration Mode*, *Site Names* display is controlled by the following *System Flags,* as in previous versions:
  — SITE_NAME_TRANSPARENCY
  — SITE_NAMES_ALWAYS_ON
  — SITE_NAMES_LOCATION

  For more information see "*Modifying System Flags"* on page **22-1**.

Site Names Display Position

The *Site Names* display position is controlled using three fields in the *Site Names* tab:

- *Display Position* drop-down menu
- *Horizontal Position* slider
- *Vertical Position* slider



Using these three fields, the position at which the *Site Names* are displayed in the *Video Windows* can be set by:

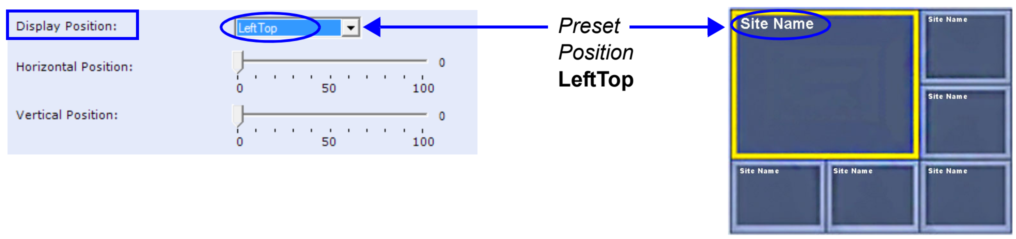
- Selecting a preset position from the drop-down menu in the *Display Position* field.
- Moving the *Horizontal* and *Vertical Position* sliders.
- Selecting **Custom** and moving the *Horizontal* and *Vertical Position* sliders.

Selecting a preset position from the drop-down menu in the Display Position field

>> In the *Display Position* drop-down menu select a preset position for *Site Names* display.
Preset positions include:

LeftTop	*Top*	*RightTop*
LeftMiddle		*RightMiddle*
LeftBottom	*Bottom*	*RightBottom*
Custom		

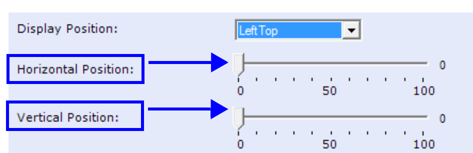
When *Custom* is selected, the current position becomes the initial position for *Site Names* position adjustments using the *Horizontal* and *Vertical Position* sliders.



The *Horizontal* and *Vertical Position* sliders are automatically adjusted to match the *Display Position* drop-down menu preset selection.

Moving the Horizontal and Vertical Position sliders

>> Drag the *Horizontal* and *Vertical Position* sliders to adjust the position of the *Site Names* display.



The *Site Names* display moves from its current position according to the slider movement.
Dragging the sliders causes the *Display Position* drop-down menu field to be set **Custom**.

Selecting Custom and moving the Horizontal and Vertical Position sliders

1 In the *Display Position* drop-down menu select **Custom**.

The current *Site Names* position becomes the initial position for *Site Names* position. Dragging the *Horizontal* and *Vertical Position* sliders moves the *Site Names* from this position.

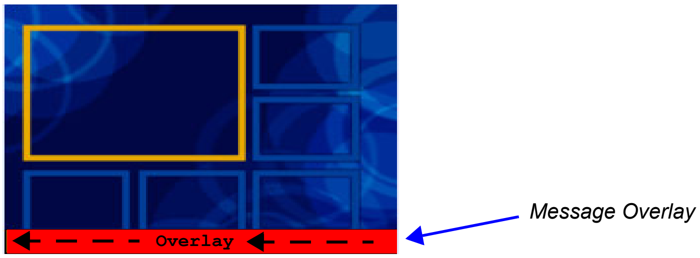
2 Drag the *Horizontal* and *Vertical Position* sliders to adjust the position of the *Site Names* display.

For a detailed description of the *Site Names* dialog box options, see Table 2-18 on page **2-42**.

Message Overlay for Text Messaging

Message Overlay allows the operator or administrator to send text messages to a single, several or all participants during an ongoing conference.

The text message is seen as part of the in the participant’s video layout on the endpoint screen or desktop display.



Guidelines

- *Message Overlay* messaging is supported in:
  — *MPM+ and MPMx Card Configuration Modes*, with a few differences in implementation between the two modes
  — Continuous Presence (CP)conferences
  — in *Same Layout* mode
  — in encrypted conferences

  It is not available for *Video Switching* (*VSW*) conferences.
- *Messages Overlay* can be enabled or disabled during the ongoing conference.
- Text messages *Content* can be changed on the fly during the ongoing conference.
- *Message Overlay* text messages are supported in *Unicode* or *ASCII* characters.
- The number of characters for each language can vary due to the type of font used, for example, the available number of characters for Chinese is 32, while for English and Russian it is 48.
  — In some languages, for example Russian, when large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.
- Changes to the *Message Overlay* display characteristics (position, size, color and speed) are immediately visible to all participants.
- Changes to the *Message Overlay Content* are immediately visible to all participants. When there is a current *Message Overlay*:
  — The current message is stopped immediately.
  — The *Display Repetition* count is reset to 1.
  — The new message *Content* is displayed <*Display Repetition*> times or until it is stopped and replaced by another *Content* change.
- If a *Repeating Message* is modified before it has completed all its repetitions, it is changed immediately without completing all of its repetitions. The modified *Repeating Message* is displayed starting with repetition one.
- *Message Overlay* messaging is not supported in *Lecture* mode.
- If during the ongoing conference the **Show Number of Participants** DTMF option (default DTMF ***88**) is used, when the displayed number of participants is removed, the message overlay text is also removed.

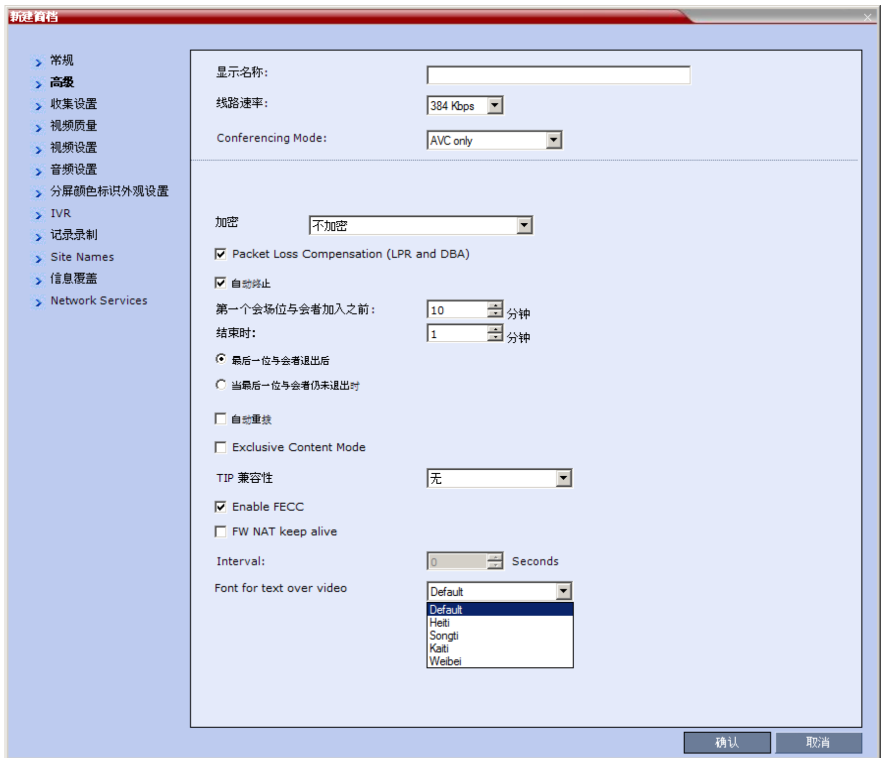
- Participants that have their video suspended do not receive *Message Overlays* messages.
- *Message Overlay* text messages cannot be sent via the *Content* channel.
- *Message Overlay* messages are not displayed when the *PCM* menu is active.
- *Message Overlay* text settings are not saved in the *Conference Template* when saving an ongoing conference as a *Conference Template*.
- Sending text messages using *Message Overlay* can be enabled or disabled during the ongoing conference. For more details, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "Sending Text Messages to All Participants Using Message Overlay (AVC-based Conferences)”* on page **3-64**.
- Text messages can be sent to individual or several participants during the ongoing conferences. For more details, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "Sending Messages to Selected Participants Using Message Overlay”* on page **3-71**.

For a detailed description of the Message Overlay parameters, see Table 2-19, “*New AVC Profile - Message Overlay Parameters,”* on page **2-46**.

Chinese Font Types

On an RMX with an MPMx card a user can select one of several Chinese fonts for use when sending text over video. New fonts can be selected with the following features:

- Site Names
- Message Overlay
- Gathering Phase Slide



New Chinese fonts available are:

- Heiti (Default)
- Songti
- Kaiti
- Weibei

This feature has the following restrictions:

- Supported on an RMX with an MPMx card(s). This feature is disabled when using an MPM+ card.
- Available when either Simplified Chinese or Traditional Chinese is selected as an available language in Setup - Customize Display Settings - Multilingual Setting. The feature is hidden if neither Simplified Chinese nor Traditional Chinese is selected.
- Only be accessed when using the RMX Web Client or the RMX Manager in Chinese.
- Available only with Continuous Presence (CP) conferences.
- Font cannot be changed during an existing conference. It can only be modified in a conference profile.

- A participant moved to another conference will be shown the font used by the new conference, even if the conferences use different fonts.

Exporting and Importing Conference Profiles

Conference Profiles can be exported from one MCU and imported to multiple MCUs in your environment, enabling you to copy the *Conference Profiles* definitions to other systems. This can save configuration time and ensures that identical settings are used for conferences running on different MCUs. This is especially important in environments using cascading conferences that are running on different MCUs.

Guidelines

- Administrators can export and import *Conference Profiles*. Operators are only allowed to export *Conference Profiles*.
- You can select a single, multiple, or all *Conference Profiles* to be exported.
- *Conference Templates* and their related *Conference Profiles* can be exported and imported simultaneously using the *Conference Templates* export and import function. For more information, see the **Exporting and Importing Conference Templates** section.

Exporting Conference Profiles

Conference Profiles are exported to a single XML file that can be used to import the *Conference Profiles* on multiple MCUs.

Using the Export Conference Profile feature, you can:

- Export all *Conference Profiles* from an MCU
- Export selected *Conference Profiles*

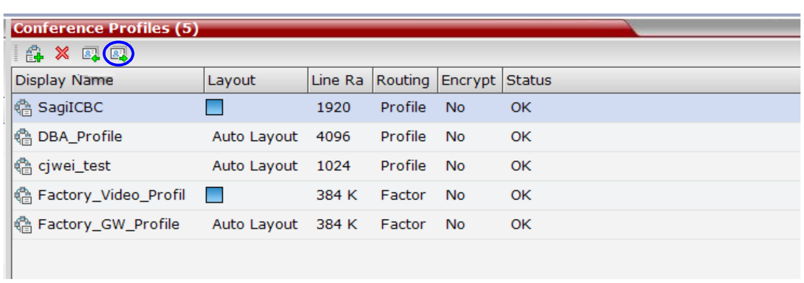
Exporting All Conference Profiles from an MCU

To export all Conference Profiles from an MCU:

1 In the *RMX Management* pane, expand the *Rarely Used* list.

2 Click the **Conference Profiles** button.

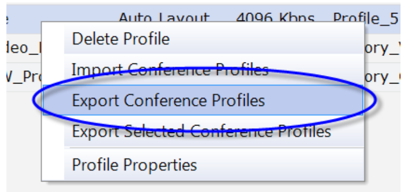
The *Conference Profiles* are displayed in the *List* pane.



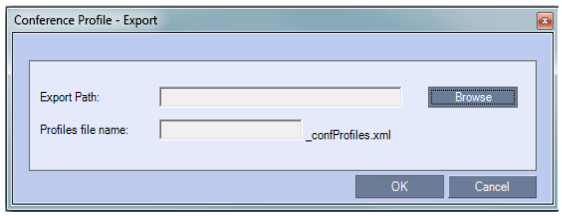
Conference Profiles (5)

Display Name	Layout	Line Ra	Routing	Encrypt	Status
SagiICBC		1920	Profile	No	OK
DBA_Profile	Auto Layout	4096	Profile	No	OK
cjwei_test	Auto Layout	1024	Profile	No	OK
Factory_Video_Profil		384 K	Factor	No	OK
Factory_GW_Profile	Auto Layout	384 K	Factor	No	OK

3 Click the **Export Conference Profiles**  button or right-click the *Conference Profiles* pane, and then click **Export Conference Profiles**.



The *Conference Profile - Export* dialog box is displayed.

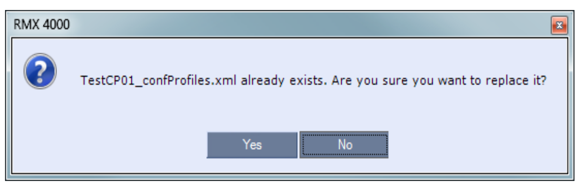


4 In the *Export Path* field, click **Browse** to navigate to the location of the desired path where you want to save the exported file.

5 In the *Profiles file name* field, type the file name prefix. The file name suffix (_confProfiles.xml) is predefined by the system. For example, if you type *Profiles01*, the exported file name is defined as *Profiles01_confProfiles.xml*.

6 Click **OK** to export the *Conference Profiles* to a file.

If the export file with the same file name already exists, a prompt is displayed.



7 Click **Yes** to replace the exported file or click **No** to cancel the export operation and return to the *Conference Profiles* list. You can modify the export file name and restart the export operation.

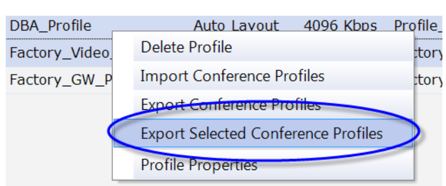
Exporting Selected Conference Profiles

You can select a single Conference Profile or multiple Conference Profiles and export them to a file to be imported to other MCUs in your environment.

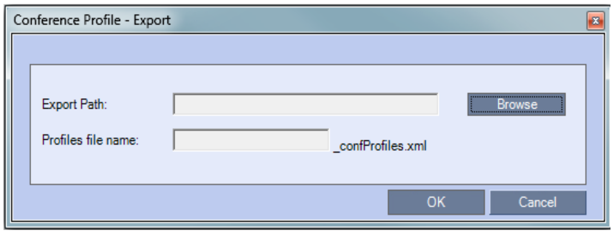
To export selected Conference Profiles:

1 In the *Conference Profiles* pane, select the profiles you want to export.

2 Right-click the selected *Conference Profiles,* and then click **Export Selected Conference Profiles**.



The *Conference Profile - Export* dialog box is displayed.

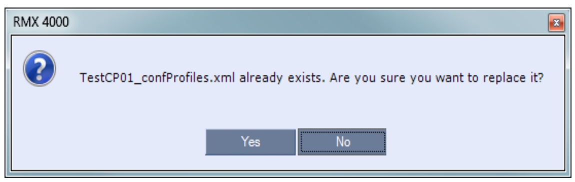


3 In the *Export Path* field, click **Browse** to navigate to the location of the desired path where you want to save the exported file.

4 In the *Profiles file name* field, type the file name prefix. The file name suffix (_confProfiles.xml) is predefined by the system. For example, if you type *Profiles01*, the exported file name is defined as *Profiles01_confProfiles.xml*.

5 Click **OK** to export the *Conference Profiles* to a file.

If the export file with the same file name already exists, a prompt is displayed.



6 Click **Yes** to replace the exported file or click **No** to cancel the export operation and return to the *Conference Profiles* list. You can modify the export file name and restart the export operation.

Importing Conference Profiles

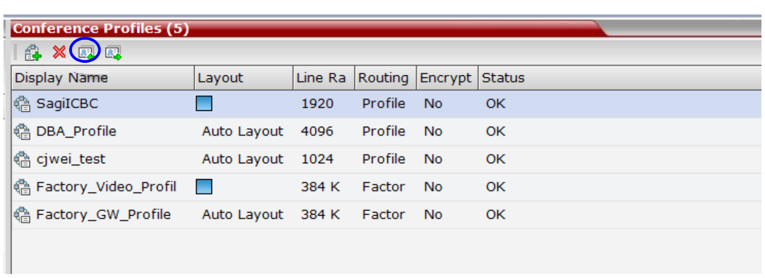
You can import Conference Profiles from another MCU in your environment.

To import Conference Profiles:

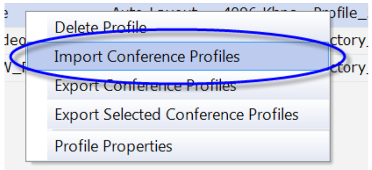
1 In the *RMX Management* pane, expand the *Rarely Used* list.

2 Click the **Conference Profiles** button.

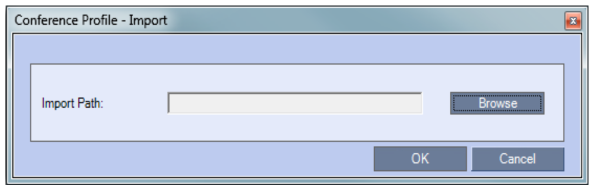
The *Conference Profiles* are displayed in the *List* pane.



3 Click the **Import Conference Profiles**  button or right-click the Conference Profiles pane, and then click **Import Conference Profiles**.



The *Conference Profile - Import* dialog box is displayed.



4 In the *Import Path* field, click **Browse** to navigate to the path and file name of the exported *Conference Profiles* you want to import.

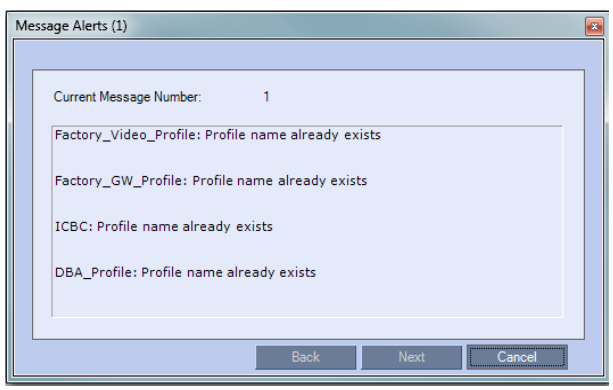
5 Click **OK** to import the *Conference Profiles*.

Conference Profiles are not imported when:

— A *Conference Profile* already exists

— An IVR Service does not exist for the related *Conference Profile*

When *Conference Profiles* are not imported into the *Conference Profiles* list, a Message Alert window is displayed with the profiles that were not imported.



Conference Profiles that are not problematic are imported.

6 Click **Cancel** to exit the *Message Alerts* window.

The imported *Conference Profiles* appear in the *Conference Profiles* list.

3

Video Protocols and Resolution Configuration for CP Conferencing

Video Resolutions in AVC-based CP Conferencing

> The following video resolution information applies to AVC Conferencing Mode.
> For a description of resolutions for SVC Conferencing Mode see "*The simulcast media streams supported by the MCU are called operation points and they are fixed for all the SVC conferences. The MCU automatically selects the operation points according to the conference line rate. Table 2-1 details the maximum resolution and frame rates supported by the MCU for each conference line rate. The actual video rate, resolution and frame rates displayed on each endpoints is determined by the endpoint's capabilities.:"* on page **2-15**.

The Polycom® RealPresence® Collaboration Server always attempts to connect to endpoints at the highest line rate defined for the conference. If the connection cannot be established using the conference line rate, the RMX attempts to connect at the next highest line rate at its highest supported resolution.

Depending on the line rate, the RMX sends video at the best possible resolution supported by the endpoint regardless of the resolution received from the endpoint.

The video resolution is also defined by the *Video Quality* settings in the *Profile*:

- **Motion**, when selected, results in lower video resolution at higher frame rates (30 fps to 60 fps).
- **Sharpness**, when selected, sends higher video resolution at lower frame rate (30 fps and lower).

The combination of **frame rate** and **resolution** affects the number of video resources required on the MCU to support the call.

The following resolutions are supported:

- CIF 352 x 288 pixels at 30 or 60 fps.
- SD 720 x 576 pixels at 30 or 60 fps.
- HD 720p 1280 x 720 pixels at 30 or 60 fps.
- HD 1080p 1920 x 1080 pixels at 30 fps
- HD 1080p 1920 x 1080 pixels at 60 fps

Video Display with CIF, SD and HD Video Connections

Although any combination of CIF, SD and HD connections is supported in all CP conferences, the following rules apply:

- In a 1X1 *Video Layout*:
  - **SD:** If the speaker transmits CIF, the MCU will send CIF to all participants, including the SD participants. In any other layout the MCU will transmit to each participant at the participant's sending resolution.
  - **HD:** The MCU transmits speaker resolution (including input from HD participants) at up to SD resolution. If 1x1 is the requested layout for the entire duration of the conference, set the conference to HD *Video Switching* mode.
- In asymmetrical *Video Layouts*:
  - **SD:** A participant in the large frame that sends CIF is displayed in CIF.
  - **HD:** Where participants' *video windows* are different sizes, the RMX transmits HD and receives SD or lower resolutions.
- In panoramic *Video Layouts*:
  - **SD**: Participants that send CIF also receive CIF.
  - **HD**: the RMX transmits HD and receives SD or lower resolutions, the RMX scales images from SD to HD resolution.

H.264 High Profile Support in CP Conferences

The *H.264 High Profile* is a new addition to the *H.264* video protocol suite. It uses the most efficient video data compression algorithms to even further reduce bandwidth requirements for video data streams.

Video quality is maintained at bit rates that are up to 50% lower than previously required. For example, a 512Kbps call will have the video quality of a 1Mbps HD call while a 1Mbps HD call has higher video quality at the same (1Mbps) bit rate.

H.264 High-Profile should be used when all or most endpoints support it.

Guidelines

- *H.264 High Profile* is supported with *MPMx* cards only.
- *H.264 High Profile* is supported in *H.323, SIP* and *ISDN* networking environments.
- *H.264 High Profile* is supported in *Continuous Presence* conferences at all bit rates, video resolutions and layouts.
- *H.264 High Profile* is the first protocol declared by the RMX, to ensure that endpoints that support the protocol will connect using it.

  Setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the *H.264 High Profile.*
- For monitoring purposes, the RMX and endpoint *H.264 High Profile* capability is listed in the *Participant Properties - H.245* and *SDP* tabs for *H.323* participants and *SIP* participants respectively.
  For more information see "*IP Participant Properties"* on page **13-22**.
- *H.264 High Profile* is not supported:
  - In *MPM* and *MPM+* card *Configuration Modes*

- For *Content Sharing*
- As an *RSS Recording* link
- With *Video Preview*

- HD1080p60 is supported
  - In *Continuous Presence* (*CP*) mode:
    - At bit rates of up to 4Mbps.
    - *HD1080p60* is supported asymmetrically: The RMX receives *HD720p60* and sends *HD1080p60*.
    - *HD1080p60* is only selectable when *Video Quality* is set to **Motion.** System behavior when *Video Quality* is set to **Sharpness** is unchanged.
  - In *Video Switching* (*VSW*) mode:
    - At bit rates of up to 6Mbps.
    - *HD1080p60* is supported symmetrically: The RMX receives and sends *HD1080p60*.
- In *Telepresence* environments the RMX sends *HD1080p60* to all endpoints except for those with *1x1 Video Layouts*, which receive the same resolution and frame rate from the RMX as they send. TIP endpoints are not supported
- PAL endpoints are supported at a frame rate of 50 fps.
- Each *HD1080p60* participant consumes 9 system resources.
  (For comparison: Each *HD720p60* participant consumes 6 system resources.)
- *HD1080p60* is not supported:
  - For *ISDN* participants.
  - For *Content* sharing.
  - With *RTV*

CP Conferencing with H.263 4CIF

The video resolution of 4CIF in H.263 endpoints is only supported for conferences in which the video quality is set to sharpness and for line rates of 384 Kbps to 1920 Kbps as shown in Table 3-1.

Table 3-1 *Video Quality vs. Line Rate*

Endpoint Line Rate Kbps	Video Quality			
	Motion		Sharpness	
	Resolution	Frame Rate	Resolution	Frame Rate
128	QCIF	30	CIF	30
256	CIF	30	CIF	30
384 - 1920+	CIF	30	4CIF	15

The RMX Web Client supports monitoring of H.263 4CIF information. The H.245 or SDP tab includes the additional information.

The creation of a new H.263 4CIF slide is supported in the IVR Service in addition to the current H.263 IVR slide. If users utilize the default Polycom slides that are delivered with RMX 1500/2000/4000, the slide's resolution will be as defined in the profile, i.e. SD, HD, CIF, etc.

For more information see "*High Resolution Slides*" on page **17-16**.

H.263 4CIF Guidelines

- H.263 4CIF is supported with H.323, SIP and ISDN connection endpoints.
- H.263 4CIF is supported in CP mode only.
- Click & View is supported in H.263 4CIF.
- AES encryption is supported with H.263 4CIF.
- H.263 4CIF is supported in recording by the RSS2000 and other recording devices.
- All video layouts are supported in H.263 4CIF, except 1x1 layout. In a 1x1 layout, the resolution will be CIF.
- For information about Resource Usage see Table 21-5 on page **21-8**.
- H.239 is supported in H.263 4CIF and is based on the same bandwidth decision matrix as for HD.

The CP Resolution Decision Matrix

All the CP resolution options and settings are based on a decision matrix which matches video resolutions to connection line rates, with the aim of providing the best balance between resource usage and video quality at any given line rate.

The following factors affect the decision matrices:

- The Media cards installed in the system affect the number of video resources used for each video resolution and frame rate, the supported video protocols and the maximum resolution that can be used by the RMX. For example, 1080p 30fps resolution is supported only with *MPM+* and *MPMx* media cards and not by *MPM* cards.
- The used video protocol: *H.264 base Profile* or H*.264 High Profile*. The *H.264 High Profil*e maintains the Video quality at bit rates that are up to 50% lower than previously required. For example, a 512 kbps call will have the video quality of a 1Mbps HD call while a 1Mbps HD call has higher video quality at the same (1Mbps) bit rate.

  H.264 High Profile is supported only by *MPMx* media cards.
- A different decision matrix is used for *Motion* and *Sharpness* as the quality requirements are different.

By default, the system shipped with three pre-defined settings of the decision matrix for H.264 *Base Profile* and three pre-defined settings of the decision matrix for *H.264 High Profile* with Motion and Sharpness video quality for each:

- **Resource-Quality Balanced (default)**

  A balance between video quality and resource usage. This is the only available resolution configuration in version 6.0.x and earlier.
- **Resource Optimized**

  System resource usage is optimized by allowing high resolution connections only at high line rates and may result in lower video resolutions (in comparison to other resolution configurations) for some line rates. This option allows to save MCU resources and increase the number of participant connections.

- **Video Quality Optimized**

  Video is optimized through higher resolution connections at lower line rates increasing the resource usage at lower line rates. This may decrease the number of participant connections.

Video Resource Usage

Video resource usage is dependent on the participant's line rate, resolution and *Video Quality* settings.

H.264 Base Profile Decision Matrix

The following illustrations show the resolutions used for the various *Line Rates* for each of the pre-defined optimization settings for *H.264 Base Profile* and *Video Quality* setting *Sharpness* and *Motion* for *MPM+* and *MPMx Card Configuration Modes*.

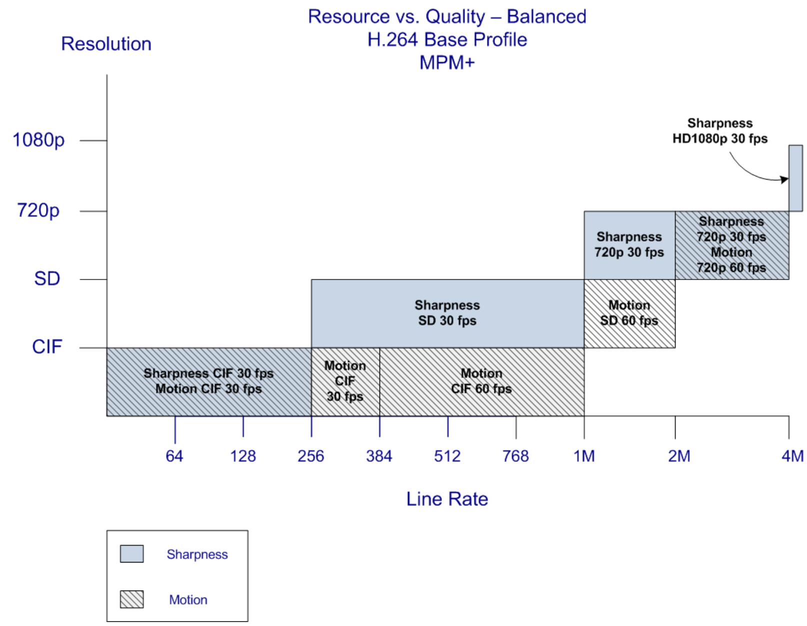


Figure 3-1 *Resolutions used per Line Rates When Resolution Configuration is set to Resource-Quality Balanced Configuration in Sharpness and Motion Mode, MPM+*

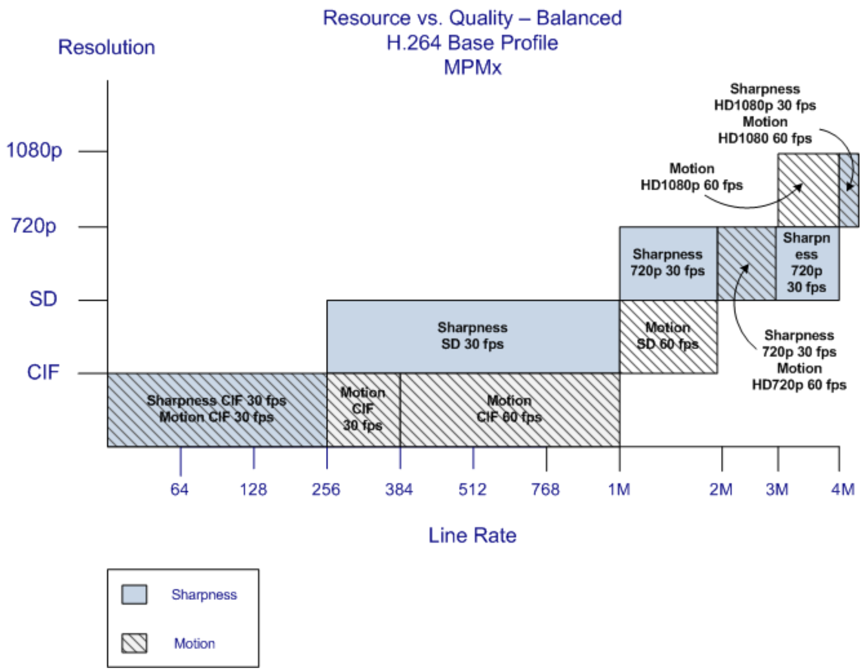


Figure 3-2 *Resolutions used per Line Rates When Resolution Configuration is set to Resource-Quality Balanced Configuration in Sharpness and Motion Mode, MPMx*

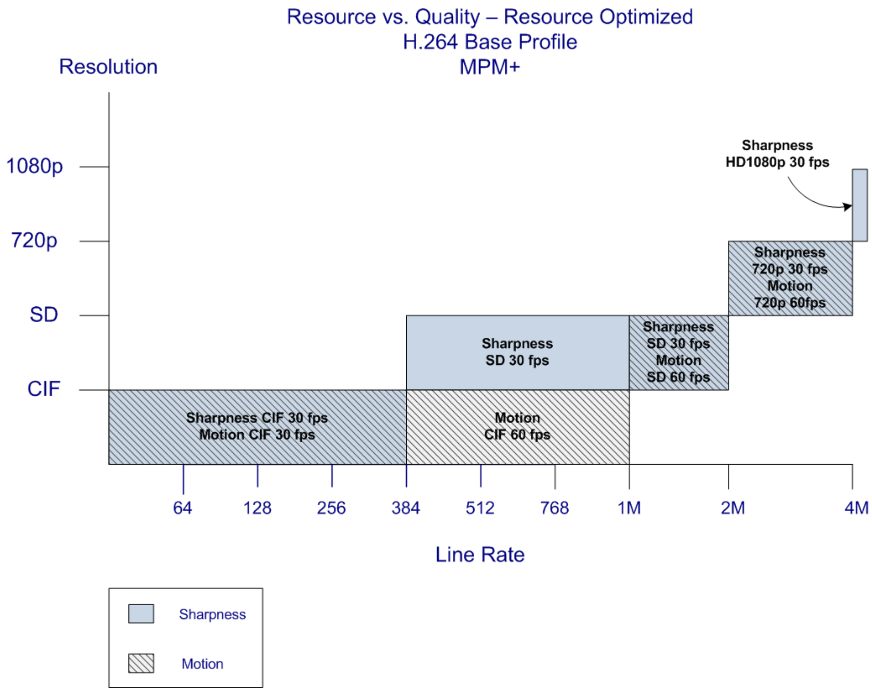


Figure 3-3 *Resolutions used per Line Rates When Resolution Configuration is set to Resource Optimized Configuration in Sharpness and Motion Mode, MPM+*

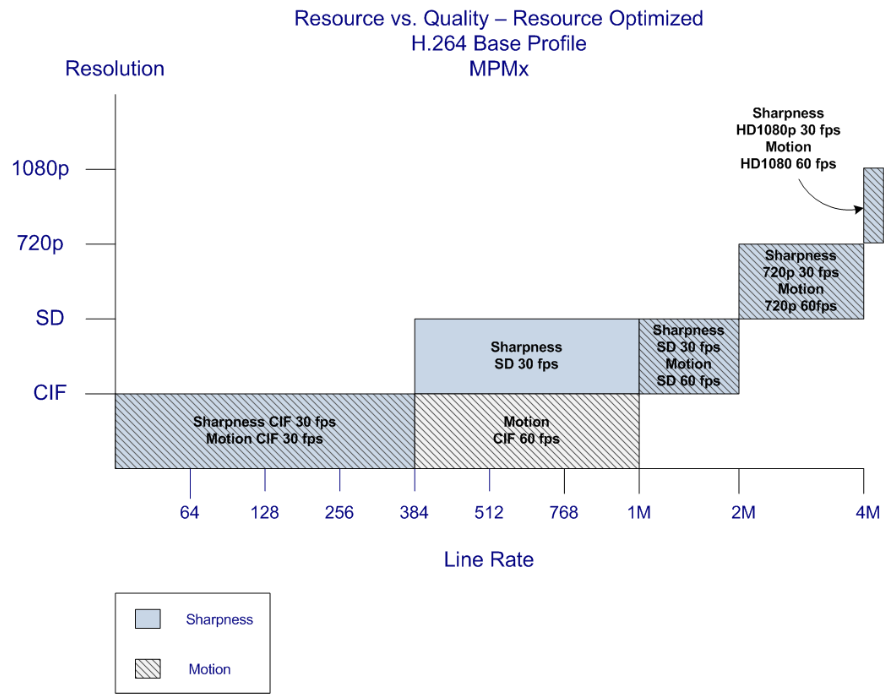


Figure 3-4 *Resolutions used per Line Rates When Resolution Configuration is set to Resource Optimized Configuration in Sharpness and Motion Mode, MPMx*

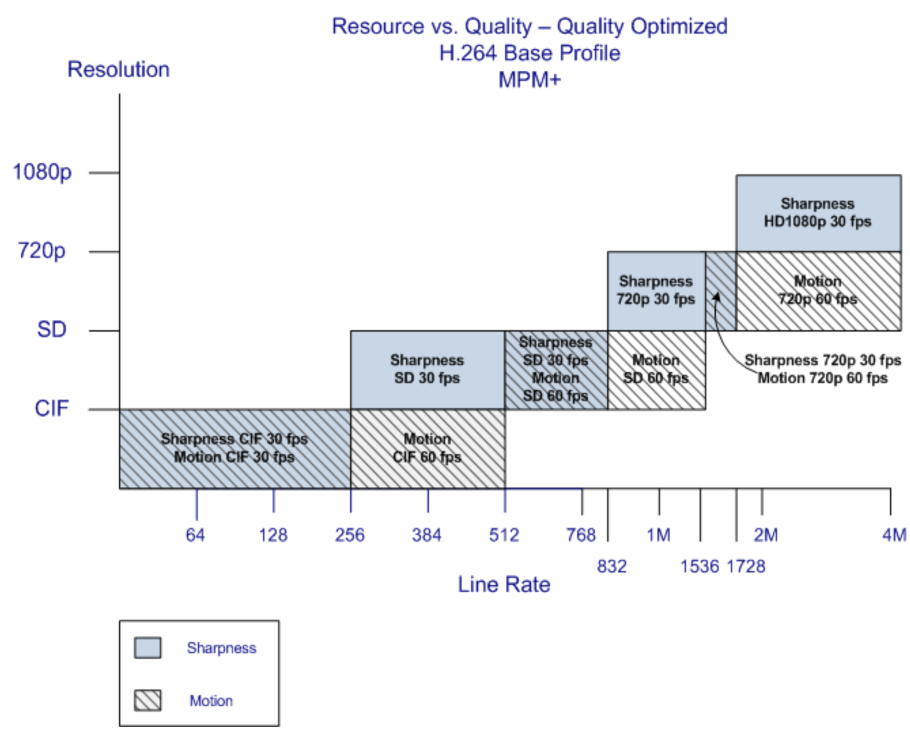


Figure 3-5 *Resolutions used per Line Rates When Resolution Configuration is set to Quality Optimized Configuration in Sharpness and Motion Mode, MPM+*

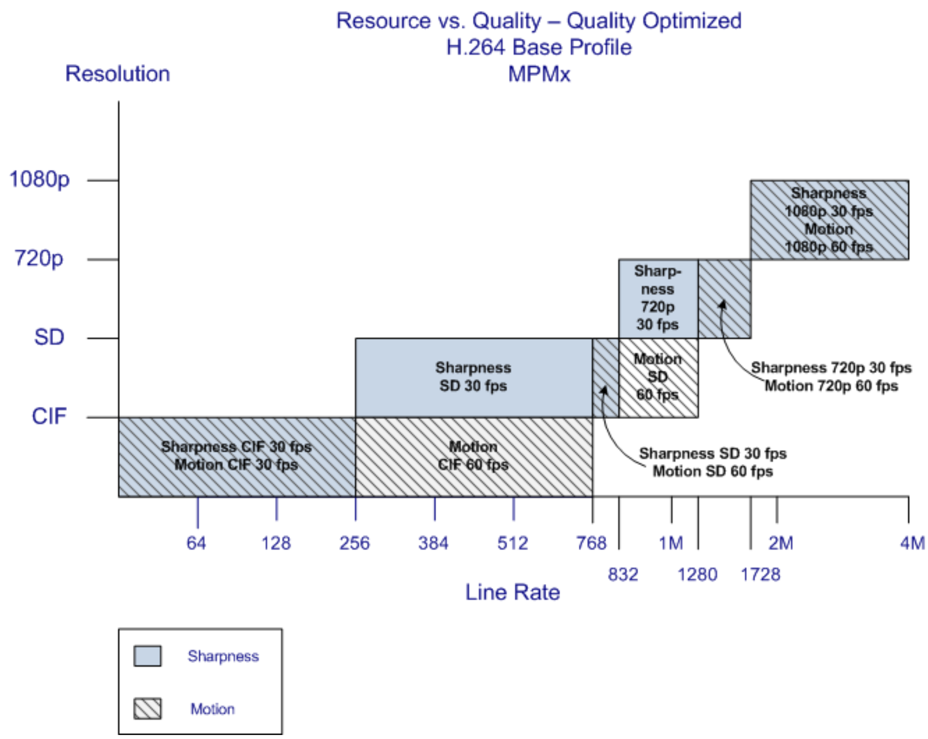


Figure 3-6 *Resolutions used per Line Rates When Resolution Configuration is set to Quality Optimized Configuration in Sharpness and Motion Mode, MPMx*

H.264 High Profile Decision Matrices (MPMx)

The following illustrations show the resolutions used for the various *Line Rates* for each of the pre-defined optimization settings for *H.264 High Profile* and *Video Quality* setting *Sharpness* and *Motion* for *MPMx Card Configuration Mode*.

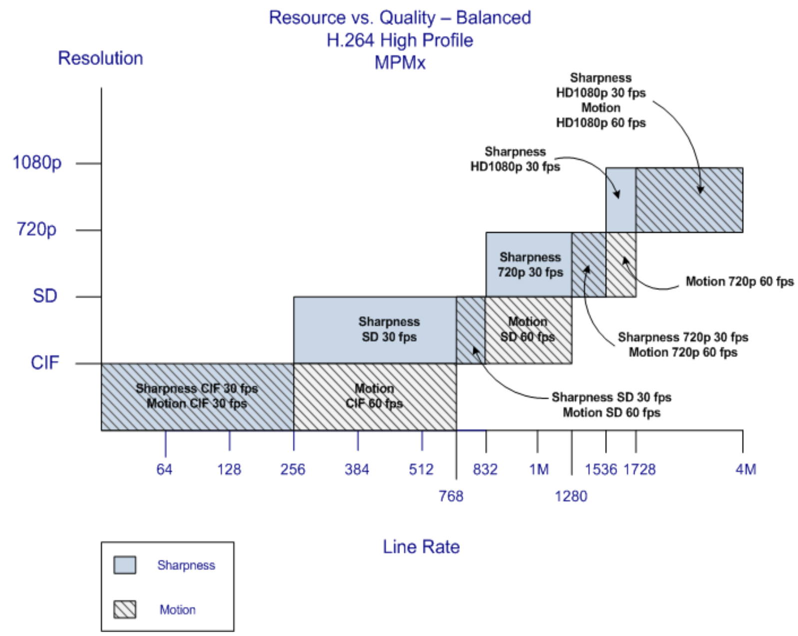


Figure 3-7 *Resolutions used per Line Rates When Resolution Configuration is set to Resource-Quality Balanced Configuration in Sharpness and Motion Mode, MPMx*

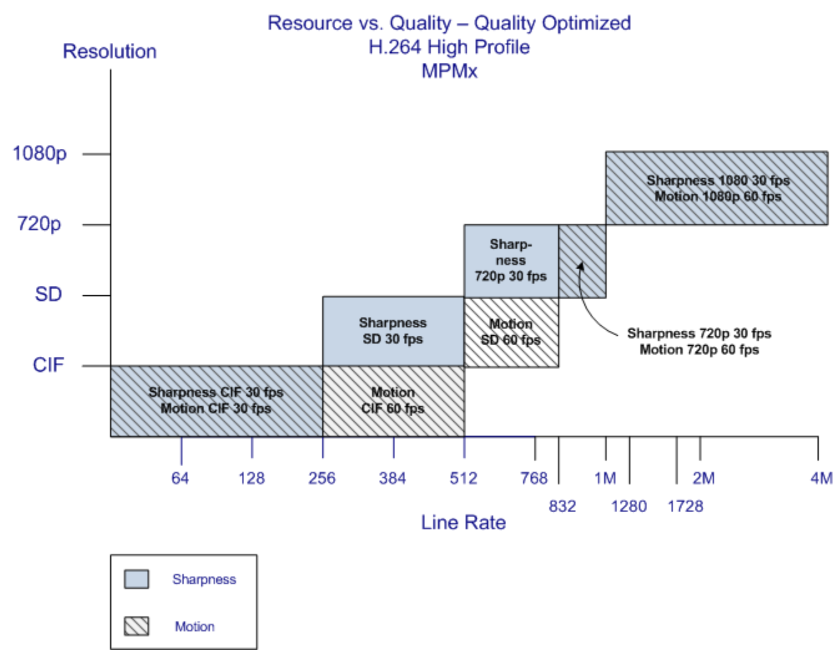


Figure 3-8 *Resolutions used per Line Rates When Resolution Configuration is set to Quality Optimized Configuration in Sharpness and Motion Mode, MPMx*

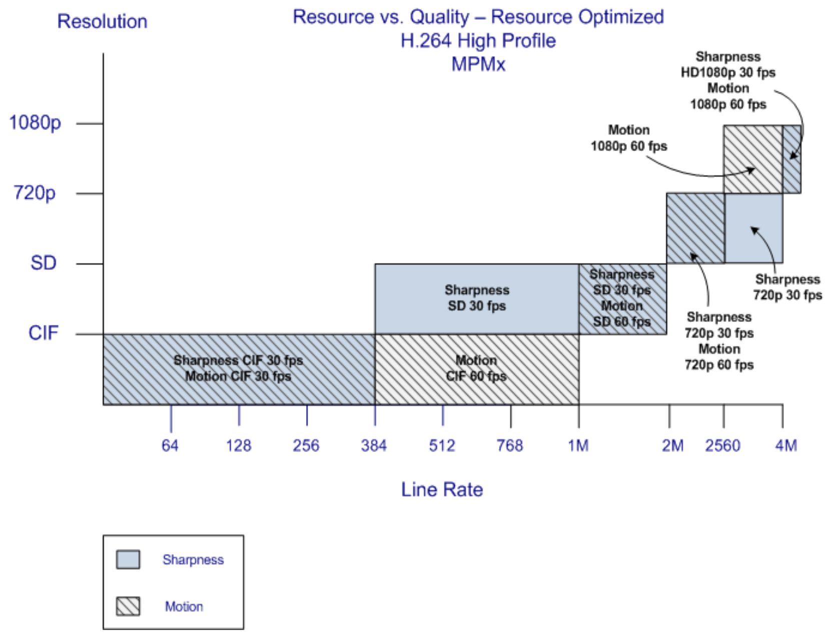


Figure 3-9 Resolutions used per Line Rates When Resolution Configuration is set to Resource Optimized Configuration in Sharpness and Motion Mode, MPMx

H.264 Base Profile and High Profile Comparison

The following illustrations show a comparison between the resolutions used at various line rates for H.264 baseline and the H.264 High Profile, for Motion and Sharpness Video Quality setting according to the *Resolution Configuration Mode* (*Balanced, Resource Optimized* or *Video Quality Optimized*).

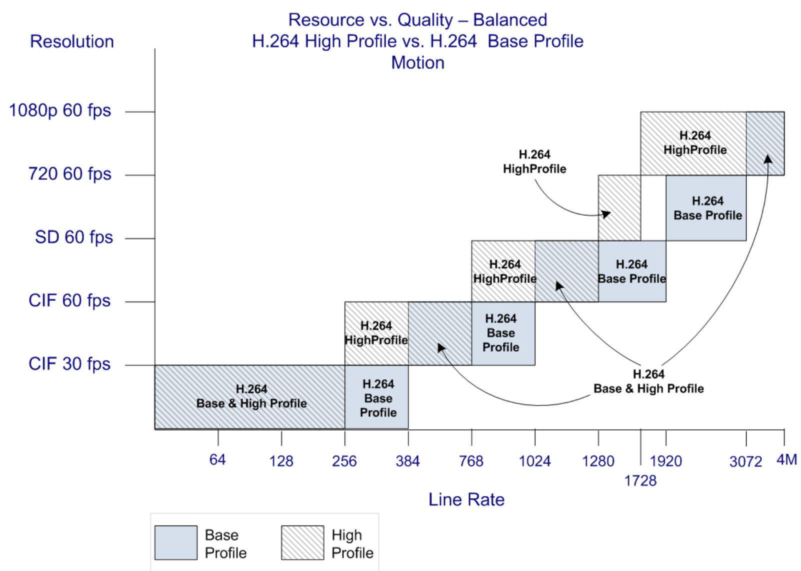


Figure 3-10 Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Resource-Quality Balanced

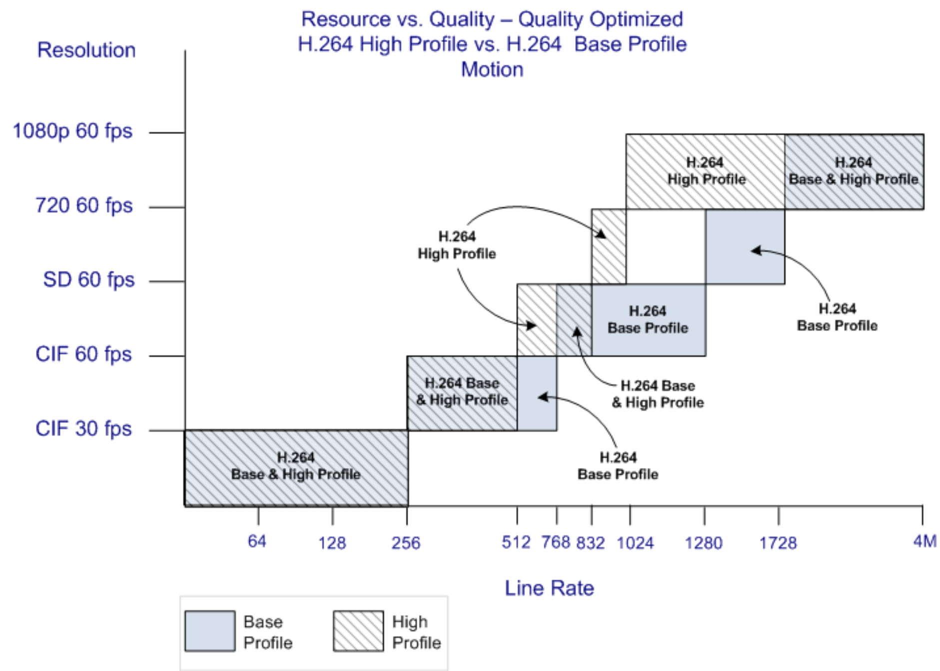


Figure 3-11 *Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Video Quality Optimized*

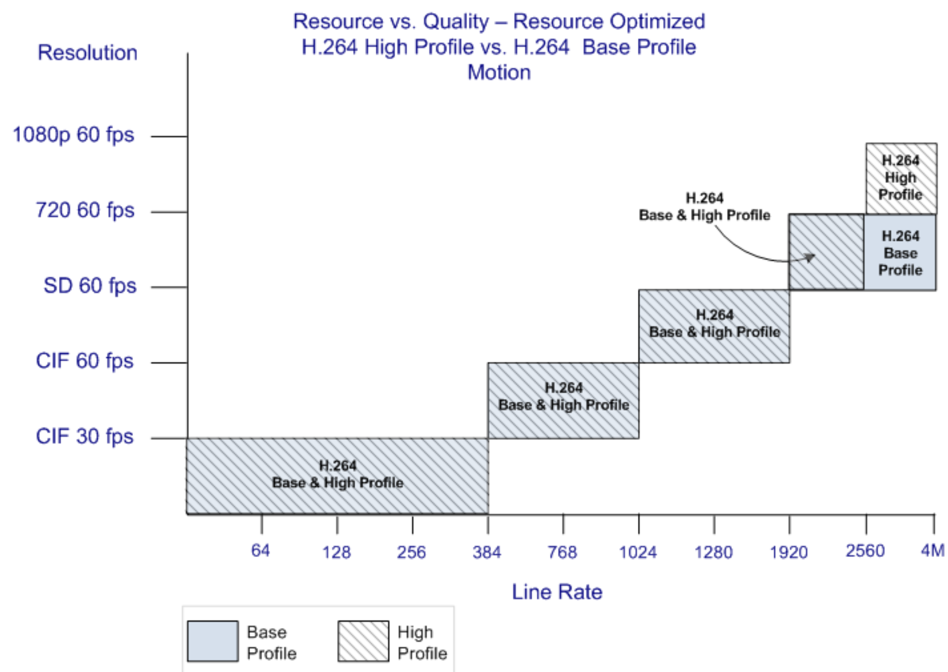


Figure 3-12 *Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Resource Optimized*

Default Minimum Threshold Line Rates and Resource Usage Summary

The following Table summarizes the *Default Minimum Threshold Line Rates* and *Video Resource* usage for each of the pre-defined optimization settings for each *Resolution*, *H.264 Profile*, *Video Quality* setting (*Sharpness* and *Motion)* for *MPM, MPM+* and *MPMx Card Configuration Modes*.

Default Minimum Threshold (kbps) by Resolution, Profile, Resources			Resource-Quality Balanced (Default)						Resource Optimized						Video Quality Optimized					
			Sharpness			Motion			Sharpness			Motion			Sharpness			Motion		
		Profile	MPM	MPM+	MPMx	MPM	MPM+	MPMx	MPM	MPM+	MPMx	MPM	MPM+	MPMx	MPM	MPM+	MPMx	MPM	MPM+	MPMx
HD1080p60	Default kbps	High						1728						2560						1024
		Base						3072						4096						1728
	Resources							9						9						9
HD1080p30	Default kbps	High			1536						4096						1024			
		Base		4096	4096					4096	4096					1728	1728			
	Resources			8	6					8	6					8	6			
HD720p60	Default kbps	High						1280						1920					1280	832
		Base					1920	1920					1920	1920					1536	1280
	Resources						8	6					8	6					8	6
HD720p30	Default kbps	High			832						1920						512			
		Base	1024	1024	1024				1920	1920	1920				832	832	832			
	Resources		4	4	3				4	4	3				4	4	3			
SD60	Default kbps	High						768						1024						768
		Base					1024	1024					1024	1024					512	768
	Resources						4	3					4	3					4	3
SD30	Default kbps	High			256						384						256			
		Base	256	256	256				384	384	384				256	256	256			
	Resources		4	2.66	1.5				4	2.66	1.5				4	2.66	1.5			
SD15	Default kbps		256						384						256					
	Resources		2						2						2					
CIF60	Default kbps	High						256						384						256
		Base					384	384					384	384					256	256
	Resources						2.66	1.5					2.66	1.5					2.66	1.5
CIF30	Default kbps	High			64			64			64			64			64			64
		Base	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64
	Resources		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

- The table above lists resource consumption for *H.264.*
- For *H.263* with *MPMx* cards:
  - CIF resolution consumes 1.5 resources.
  - 4CIF resolution consumes 3 resources.

Resolution Configuration for CP Conferences

The *Resolution Configuration* dialog box enables RMX administrators to override the default video resolution decision matrix, effectively creating their own decision matrix. The minimum threshold line rates at which endpoints are connected at the various video resolutions can be optimized by adjusting the resolution sliders.

System resource usage is also affected by the *Resolution Configuration* settings. For more information see "*Video Resource Usage"* on page **3-5** and "*Default Minimum Threshold Line Rates and Resource Usage Summary"* on page **3-12**.

Guidelines

- *Resolution Slider* settings affect all *Continuous Presence* (*CP*) conferences running on the RMX. *Video Switched* conferences are not affected.

On the RealPresence Collaboration Server (RMX) 1500 MPMx-Q assembly, the use of HD with Continuous Presence requires an additional license. In the Resource Report and Resolution Configuration panes, HD settings are displayed but are not enabled and if HD is selected the system will enable SD by default.

- A system restart is not needed after changing the *Resolution Slider* settings.
- *Resolution Slider* settings cannot be changed if there are ongoing conferences running on the RMX.
- The displayed sliders and the resolutions change according the *Card Configuration Mode: MPM, MPM*+ or *MPMx.*

From *Version 7.1*, *MPM* media cards are not supported.

Accessing the Resolution Configuration Dialog Box

The *Resolution Configuration* dialog box is accessed by clicking **Setup > Resolution Configuration** in the *RMX Setup* menu.

The *Resolution Configuration* dialog box display changes according to the *Card Configuration Mode*:

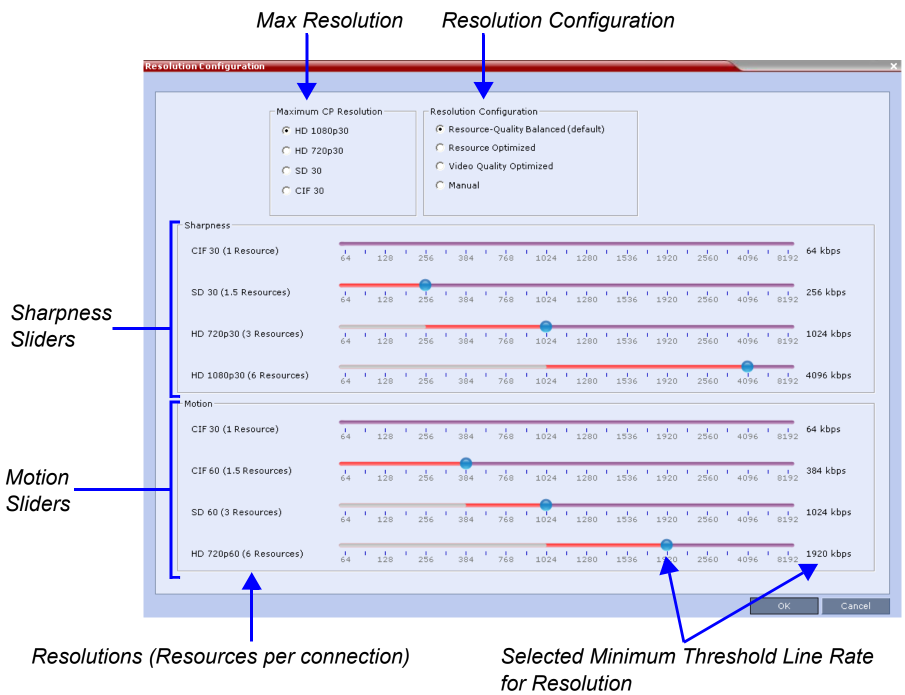
- *MPM* and *MPM+*
- *MPMx* - supports *H.264 High Profile*

Modifying the Resolution Configuration in MPM or MPM+ Card Configuration Mode

The *Resolution Configuration* dialog box shown below is displayed when the RMX is in *MPM*, *MPM+* or *MPMx Card Configuration Mode*.

The *Resolution Configuration dialog* box opens. It contains the following elements:

- *Maximum CP Resolution Pane*
- *Resolution Configuration Pane*
- *Sharpness Resolution Sliders*
- *Motion Resolution Sliders*



Maximum CP Resolution Pane

Depending on the media cards installed, the *Maximum CP Resolution* of the RMX can be set to one of the following resolutions:

MPM Cards	MPM+ Cards	MPM+ Cards
HD 720p30	HD 1080p30	HD 1080p60
SD 30	HD 720p30	HD 1080p30
SD 15	SD 30	HD 720p30
CIF 30	CIF 30	SD 30
		CIF 30

Limiting Maximum Resolution

Before a selection is made in this pane, the *Maximum CP Resolution* of the system is determined by the **MAX_CP_RESOLUTION** System Flag.

The **MAX_CP_RESOLUTION** flag value is applied to the system during *First Time Power-on* and after a system upgrade. The default value is *HD1080p60*.

All subsequent changes to the *Maximum CP Resolution* of the system are made by selections in this pane.

Maximum Resolution

Maximum Resolution can be limited per **conference** or per **participant endpoint**.

The *Maximum Conference Resolution*, can be limited via the *Profile - Video Quality* dialog box. For more information see "*Defining New Profiles"* on page **2-18**.

The *Maximum Resolution* can further be limited per participant endpoint via the *Participant - Properties* dialog box. For more information see "*Managing the Address Book"* on page **8-7**.

Resolution Configuration Pane

The user can select from 3 pre-defined *Resolution Configurations* or select a manual *Resolution Slider* adjustment mode. The pre-defined settings can be accepted without modification or be used as the basis for manual fine tuning of resolution settings by the administrator.

The *Manual* radio button is automatically selected if any changes are made to the *Resolution Sliders*.

The *Resolution Configurations* are:

- **Resource-Quality Balanced (default)**

  A balance between the optimized video quality and optimized resource usage. This is the only available resolution configuration in version 6.0.x and earlier.

> Use this option:
> - When the priority is to maintain a balance between resource usage and video quality.
> - When it is necessary to maintain backward compatibility with previous versions.
> - When working with CMA.

  The *Balanced* settings are described in the section*:* "*The CP Resolution Decision Matrix"* on page **3-4**.

- **Resource Optimized**

  System resource usage is optimized by allowing high resolution connections only at high line rates and may result in lower video resolutions (in comparison to other resolution configurations) for some line rates.

> Use this option when the priority is to save MCU resources and increase the number of participant connections.

  The *Resource Optimized* settings are described in the section*:* "*The CP Resolution Decision Matrix"* on page **3-4**.

- **Video Quality Optimized**

  Video is optimized through higher resolution connections at lower line rates increasing the resource usage at lower line rates. This may decrease the number of participant connections.

> Use this option when the priority is to use higher video resolutions while decreasing the number of participant connections.

  The V*ideo Quality Optimized* settings are described in the section*:* "*The CP Resolution Decision Matrix"* on page **3-4**.

- **Manual**

  The administrator adjusts the sliders to accommodate local conferencing requirements.

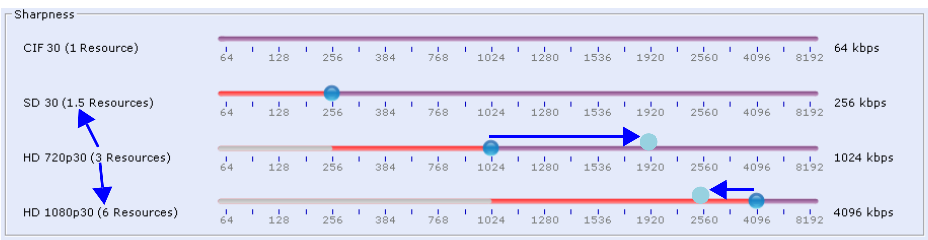
Sharpness / Motion Resolution Slider Panes

Sharpness and *Motion* are *Video Quality* settings that are selected per conference and are defined in the conference *Profile* and they determine the resolution matrix that will be applied globally to all conferences according to the selection of *Sharpness* or *Motion*. The resolution matrix for *Sharpness* or *Motion* is determined by the resolution configuration and can be viewed in the *Resolution Configuration* sliders.

System Resource usage is affected by the *Resolution Configuration* settings.

Example

As shown in following diagram:



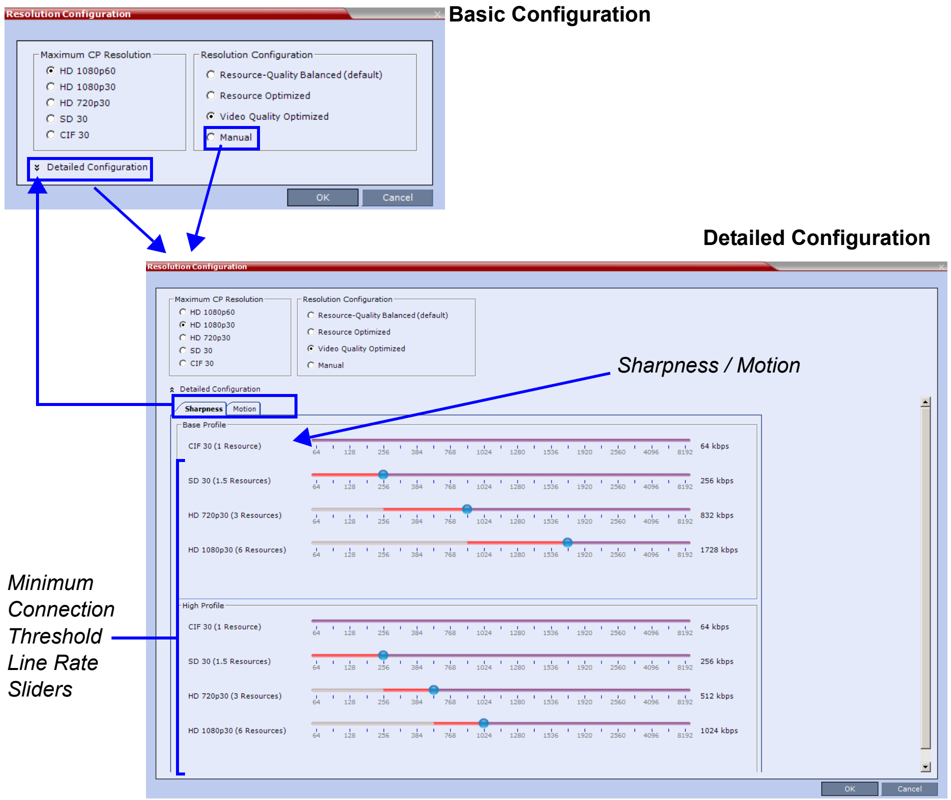
- Moving the *HD720p30* resolution slider from 1024kbps to 1920kbps increases the minimum connection threshold line rate for that resolution. Endpoints connecting at line rates between 1024kbps and 1920kbps that would have connected at *HD 720p30* resolution will instead connect at *SD 30* resolution. Each of the affected endpoints will connect at lower resolution but will use 1.5 system resources instead of 3 system resources.
- Moving the *HD1080p30* resolution slider from 4096kbps to 2560kbps decreases the minimum connection threshold line rate for that resolution. Endpoints connecting at line rates between 2560kbps and 4096kbps that would have connected at *HD 720p30* resolution will instead connect at *HD 1080p30* resolution. Each of the affected endpoints will connect at higher resolution but will use 6 system resources instead of 3 system resources.

Modifying the Resolution Configuration in MPMx Card Configuration Mode

The *Resolution Configuration - Basic Configuration* dialog box is the first dialog box displayed when the RMX is in *MPMx Card Configuration Mode.*

Clicking the **Detailed Configuration** button toggles the display of the *Detailed Configuration* pane, which displays sliders for modifying minimum connection threshold line rates for endpoints that support *H.264 Base Profile* or *High Profile*. The *Detailed Configuration* pane can also be opened by clicking the **Manual** radio button in the *Resolution Configuration* pane.

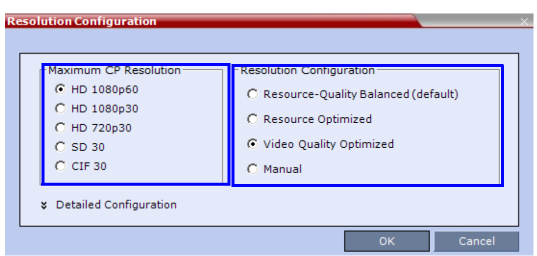
Sharpness and *Motion* settings are accessed by clicking the **Sharpness** and **Motion** tabs when the *Detailed Configuration* is open.



Resolution Configuration - Basic

The *Resolution Configuration -Basic* dialog box contains the following panes:

- *Max CP Resolution Pane*
- *Resolution Configuration Pane*



Maximum CP Resolution Pane

In *MPMx Card Configuration Mode* the RMX can be set to one of the following *Maximum CP Resolutions*:

- HD 1080p60
- HD 1080p30
- HD 720p30
- SD 30
- CIF 30

Limiting Maximum Resolution

Before a selection is made in this pane, the *Maximum CP Resolution* of the system is determined by the **MAX_CP_RESOLUTION** *System Flag*.
For more information see "*Limiting Maximum Resolution"* on page **3-15**.

Resolution Configuration Pane

The *Resolution Configuration* pane and its selection options in *MPMx Card Configuration Mode* behave in the same manner as for *MPM* and *MPM+ Card Configuration Modes* as described in the *"Resolution Configuration Pane"* section on page **3-15**.

Resolution Configuration - Detailed

H.264 High Profile allows higher quality video to be transmitted at lower bit rates.

However, setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the *H.264 High Profile*. The RMX uses two decision matrices (*Base Profile*, *High Profile)* to enable endpoints to connect according to their capabilities.

Sharpness and Motion

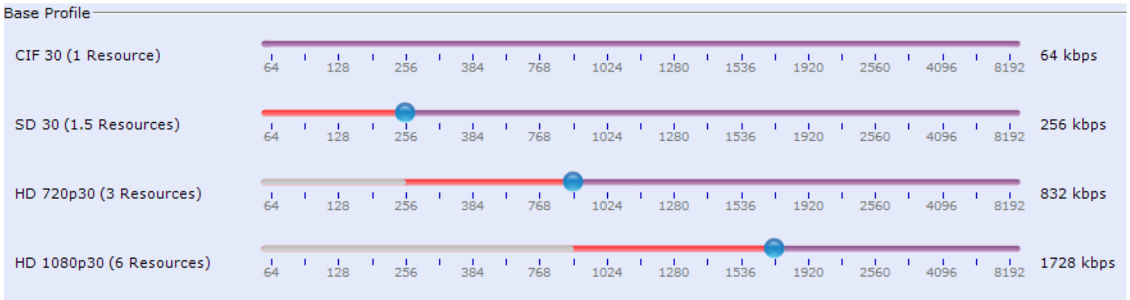
Sharpness and *Motion* are *Video Quality* settings that are selected per conference and are defined in the conference *Profile.* A conference with *Sharpness* selected in its *Profile* uses the *Sharpness* settings of the *Resolution Configuration* and a conference with *Motion* selected in its *Profile* uses the *Motion* settings of the *Resolution Configuration* dialog box.

The *Sharpness* and *Motion* tabs in the *Resolution Configuration* dialog box allow the user to view and modify *Resolution Configuration* settings for conferences with either *Video Quality* setting.

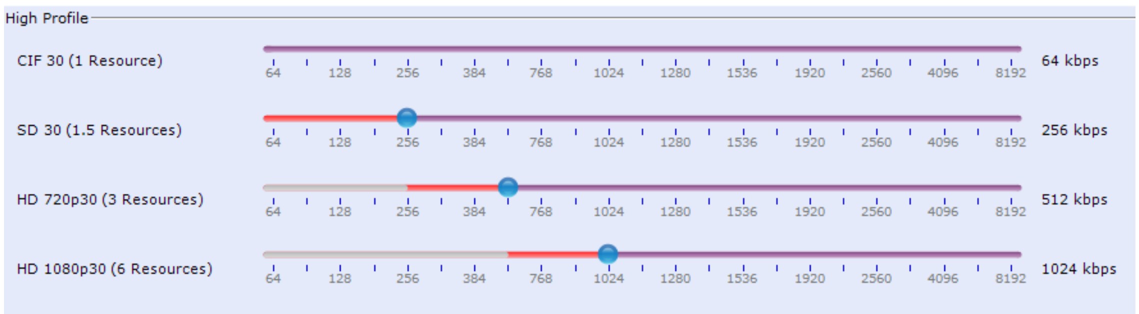
Resolution Configuration Sliders

The *Detailed Configuration* dialog box allows the administrator to configure minimum connection threshold bit rates for endpoints that support *H.264 High Profile* and those that do not support *H.264 High Profile* by using the following slider panes:

- Base Profile - Endpoints that do not support H.264 High Profile connect at these minimum threshold bit rates.



- *High Profile* - Endpoints that support *H.264 High Profile* connect at these minimum threshold bit rates.



Although the default minimum threshold bit rates provide acceptable video quality, the use of higher bit rates usually results in better video quality.

Base Profile / High Profile Resolution Slider Panes

The *Base Profile* and *High Profile* sliders operate in the same manner as that described for the *Sharpness* and *Motion* sliders. For more information see the example in the section: "*Sharpness / Motion Resolution Slider Panes"* on page **3-16**.

Flag Settings

Setting the Maximum CP Resolution for Conferencing

The **MAX_CP_RESOLUTION** flag value is applied to the system during *First-time Power-up* and after a system upgrade. The default value is *HD1080p60*.

All subsequent changes to the *Maximum CP Resolution* of the system are made by selections in the *Max Resolution* pane of the ***Resolution Configuration*** dialog box.

Depending on the type of *Media* card(s) installed, the *Maximum CP Resolution* of the RMX can be set to one of the following resolutions:

MPM Cards	**MPM+ / MPMx Cards**
HD 720p30	HD 1080p60
SD 30	HD 720p30
SD 15	SD 30
CIF 30	CIF 30

Minimum Frame Rate Threshold for SD Resolution

The **MINIMUM_FRAME_RATE_THRESHOLD_FOR_SD** *System Flag* can be added and set to prevent low quality, low frame rate video from being sent to endpoints by ensuring that an *SD* channel is not opened at frame rates below the specified value. For more information see "*Modifying System Flags"* on page **22-1**.

H.264 High Profile System Flags (Version 7.0.1 only)

The flags listed below are used in version 7.0.1 only. From *Version 7.0.2* these flags were replaced with the *High Profile* sliders in the *Resolution Configuration* dialog box. For more information, see "*Controlling Resource Allocations for Lync Clients Using RTV Video Protocol"* on page **3-27**.

Setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the *H.264 High Profile.*

Endpoints that do not support *H.264 High Profile* will connect according to the minimum bitrate thresholds defined by the following *System Flags*:

- H264_BASE_PROFILE_MIN_RATE_SD30_SHARPNESS
- H264_BASE_PROFILE_MIN_RATE_HD720P30_SHARPNESS
- H264_BASE_PROFILE_MIN_RATE_HD1080P30_SHARPNESS
- H264_BASE_PROFILE_MIN_RATE_CIF60_MOTION
- H264_BASE_PROFILE_MIN_RATE_SD60_MOTION
- H264_BASE_PROFILE_MIN_RATE_HD720P60_MOTION

These *System Flags* must be added to the *System Configuration* file before they can be modified. For more information see the "*Modifying System Flags"* on page **22-1**.

Example: If the *High Profile Optimized* option is selected in the *Resolution Configuration* dialog box and the *System Flag* values are set as in the following table:

System Flag	Default Value
H264_BASE_PROFILE_MIN_RATE_SD30_SHARPNESS	256
H264_BASE_PROFILE_MIN_RATE_HD720P30_SHARPNESS	1024
H264_BASE_PROFILE_MIN_RATE_HD1080P30_SHARPNESS	1536
H264_BASE_PROFILE_MIN_RATE_CIF60_MOTION	256
H264_BASE_PROFILE_MIN_RATE_SD60_MOTION	1024
H264_BASE_PROFILE_MIN_RATE_HD720P60_MOTION	1536

Endpoints will connect at resolutions as set out in the following table, depending on whether they support *H.264 High Profile* or not:

Video Quality Setting	Endpoint Connection Bit Rate (kbps)		Resolution
	High Profile Supported	High Profile Not Supported	
Sharpness	**128**<= bit rate <**512**	**256**<= bit rate <**1024**	SD30
	512<= bit rate <**1024**	**1024**<= bit rate <**1536**	HD720p30
	1024<= bit rate	**1536**<= bit rate	HD1080p30
Motion	**128**<= bit rate <**512**	**256**<= bit rate <**1024**	CIF60
	512<= bit rate <**832**	**1024**<= bit rate <**1536**	SD60
	832<= bit rate	**1536**<= bit rate	HD720p60 HD1080p60

Additional Video Resolutions in MPM+/MPMx Card Configuration Mode

The following higher video quality resolutions are available when the RMX is working in *MPM+* or *MPMx Mode*:

- CIF 352 x 288 pixels at 50 fps.
- WCIF 512 x 288 pixels at 50 fps.
- WSD 848 x 480 pixels at 50 fps.
- W4CIF 1024 x 576 pixels at 30 fps.
- HD 720p 1280 x 720 pixels at 60 fps (symmetric with *MPMx*).
- HD 1080p 1920 x 1080 pixels at 30 fps (symmetric with *MPMx*).
- HD 1080p 1920 x 1080 pixels at 60 fps (symmetric with *MPMx*).

The video resolution transmitted to any endpoint is determined by the endpoint's capabilities, the conference line rate, the Conference Profile's Motion and Sharpness settings and the RMX's Card Configuration Mode (MPM+ or MPMx).

w448p Resolution

For improved interoperability with *Tandberg MXP 990/3000* endpoints, the appropriate *System Flag* settings, will force the RMX to send *w448p* (768x448 pixels) at 25fps as a replacement resolution for *WSD15* (848x480) and *SD15* (720x576 pixels).

Guidelines

- The *w448p* resolution is supported:
  - In *MPMx* card configuration mode.
  - In *CP* mode.
  - At conference line rates of 384kbps and 512kbps.

— With *H.323, SIP* and *ISDN* endpoints.
H.323 endpoints must identify themselves as **Tandberg MXP** during capabilities exchange.
— In all *Video Layouts*.
— In *1x1 Layout*:
- When *Video Clarity* is **Off**, the RMX transmits the same resolution as it receives.
- When *Video Clarity* is **On**, the RMX changes the transmitted resolution to *w448p*.

For more information see page 2-9.

- Resource consumption for the w*448p* resolution is the same as for *SD* and *WSD* resolutions, with each *MPMx-D* card supporting up to 60 *w448p* participants.

The following table lists the video outputs from the RMX to the *Tandberg Endpoints* for both *16:9 Aspect Ratio* when the w*448p* resolution is enabled.

Table 3-2 *Video Output to Tandberg Endpoints- Aspect Ratio 16:9*

Network Environment	Video Quality		Line Rate Kbps	Resolution	Frame Rate fps	Resolution	Frame Rate fps
	Tandberg	RMX		Tandberg to RMX		RMX to Tandberg	
H.323 SIP ISDN	Motion	Sharpness	384	512x288	30	**768x448**	**25**
			512	768x448	30	**768x448**	**25**
H.323 SIP ISDN	Sharpness*	Sharpness	384	1024x576	15	**768x448**	**25**
			512	1024x576	15	**768x448**	**25**

* It is recommend to set the endpoint to **Motion** to ensure the transmission of the higher frame rates of 25fps/30fps to the RMX.

The following table list the video outputs from the RMX to the *Tandberg Endpoints* for *4:3 Aspect Ratio* when the w*448p* resolution is enabled.

Table 3-3 *Video Output to Tandberg Endpoints - Aspect Ratio 4:3*

Network Environment	Video Quality		Line Rate Kbps	Resolution	Frame Rate fps	Resolution	Frame Rate fps
	Tandberg	RMX		Tandberg to RMX		RMX to Tandberg	
H.323 SIP ISDN	Motion	Sharpness	384	576x448 ‡	25	**768x448**	**25**
			512	576x448 ‡	25	**768x448**	**25**
H.323 SIP ISDN	Sharpness*	Sharpness	384	4CIF	15	**768x448**	**25**
			512	4CIF	15	**768x448**	**25**

* It is recommend to set the endpoint to **Motion** to ensure the transmission of the higher frame rates of 25fps/30fps to the RMX.

‡ *MXP 990/3000* endpoints transmit 576x448 pixels. Other *MXP* endpoints may transmit other resolutions eg. *CIF*.

Content

Sharing and receiving *Content* is supported.

Bandwidth allocated to the *Content* channel during *Content* sharing may cause the video resolution to be decreased as from *w448p* to *w288p*.

When *Content* sharing stops and the full bandwidth becomes available, video resumes at the previous *w448p* resolution.

For more information see "*H.239"* on page **4-2**.

Packet Loss Compensation

If there is *Packet Loss* in the network and *Dynamic Bandwidth Allocation* (*DBA*) is activated, allocating bandwidth for *Lost Packet Recovery,* video resolution decreases from *w448p* to *w288p*.

When *Packet Loss* ceases and *DBA* no longer needs to allocate bandwidth for *Lost Packet Recovery*, the full bandwidth becomes available and video resumes at the previous *w448p* resolution.

For more information see "*Packet Loss Compensation (LPR and DBA)"* on page **4-50**.

Enabling Support of the w448p Resolution

w448p resolution support for *Tandberg* endpoints requires setting of the following entities:

- *Tandberg* endpoint
- RMX flags
- *RMX Conference Profile*

RMX System Flag Settings

- The *System Flag* **USE_INTERMEDIATE_SD_ RESOLUTION** must be manually added to *system.cfg* with its value set to **YES**.
- The value of the **PAL_NTSC_VIDEO_OUTPUT** *System Flag* must be set to **PAL**.

  If the *System Flag* is not defined as **PAL**, and if the current speaker is sending **NTSC** video stream, the *frame rate* will decrease to 15fps. Setting the flag to **PAL** will ensure that a *frame rate* of 25fps is maintained.

For more information about modifying *System Flags,* see "*Modifying System Flags"* on page **22-1**.

SIP and ISDN endpoints

The *System Flag* only affects endpoints that support *SD* resolution and for which the RMX would have selected a transmission frame rate of 15 fps. Higher resolution endpoints are not affected by this flag.

All *SIP* and ISDN endpoints (not only *Tandberg MXP*) are connected as if they are *Tandberg MXP* causing the RMX to select *w448p*, because endpoint-type information from these endpoints is not guaranteed during capabilities exchange.

> For flag changes (including deletion) to take effect, the RMX must be reset. For more information, see the "*Resetting the RMX"* on page **21-69**.

RMX Profile Setting

- On the RMX, the *Video Quality* field in the *New Profile - Video Quality* dialog box must be set to **Sharpness**.
  For more information see , "*Defining New Profiles"* on page **2-18**.

Additional Intermediate Video Resolutions

Two higher quality, intermediate video resolutions replace the transmission of CIF (352 x 288 pixels) or SIF (352 x 240 pixels) resolutions to endpoints that have capabilities between:

- **CIF** (352 x 288 pixels) and **4CIF** (704 x 576 pixels) – the resolution transmitted to these endpoints is **432 x 336** pixels.
- **SIF** (352 x 240 pixels) and **4SIF** (704 x 480 pixels) – the resolution transmitted to these endpoints is **480 x 352** pixels.

The frame rates (depending on the endpoint's capability) for both intermediate resolutions are:

- In *MPM Mode* – 25 or 30 fps.

In *MPM+ / MPMx Mode* – 50 or 60 fps.

For information about setting system flags, see "*Controlling Resource Allocations for Lync Clients Using RTV Video Protocol"* on page **3-27**.

Microsoft RTV Video Protocol Support in CP Conferences

Microsoft RTV (*Real Time Video*) protocol provides high quality video conferencing capability to *Microsoft OC* (*Office Communicator*) Client endpoints at resolutions up to *HD720p30*. Interoperability between *Polycom HDX* and *OCS* endpoints is improved.

Guidelines

- The *RTV* protocol is supported:
  - On *RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000*
  - With *MPMx* cards
  - In *SIP* networking environments only
  - In CP mode only
- *OCS (Wave 13)* and *Lync Server (Wave 14)* clients are supported.
- *RTV* is supported in *Basic Cascade* mode.
- *RTV* is the default protocol for *OCS* endpoints and *Lync Server* clients connecting to a conference.
- *RTV* participants are supported in recorded conferences.
- *RTV* participant encryption is supported using the *SRTP* protocol.
- *Video Preview* is not supported for *RTV* endpoints.
- *Custom Slides* in *IVR Services* are not supported for *RTV* endpoints.

- *HD720p30* resolution is supported at bit rates greater than 600 kbps. The following table summarizes the resolutions supported at the various bit rates.

Table 3-4 RTV - Resolution by Bit Rate

Resolution	Bitrate
QCIF	**Bitrate** <180kbps
CIF30	180kbps < **Bitrate** < 250kbps
VGA (SD30)	250kbps < **Bitrate** < 600kbps *
HD720p30	600kbps < **Bitrate** *

* Dependant on the PC's capability

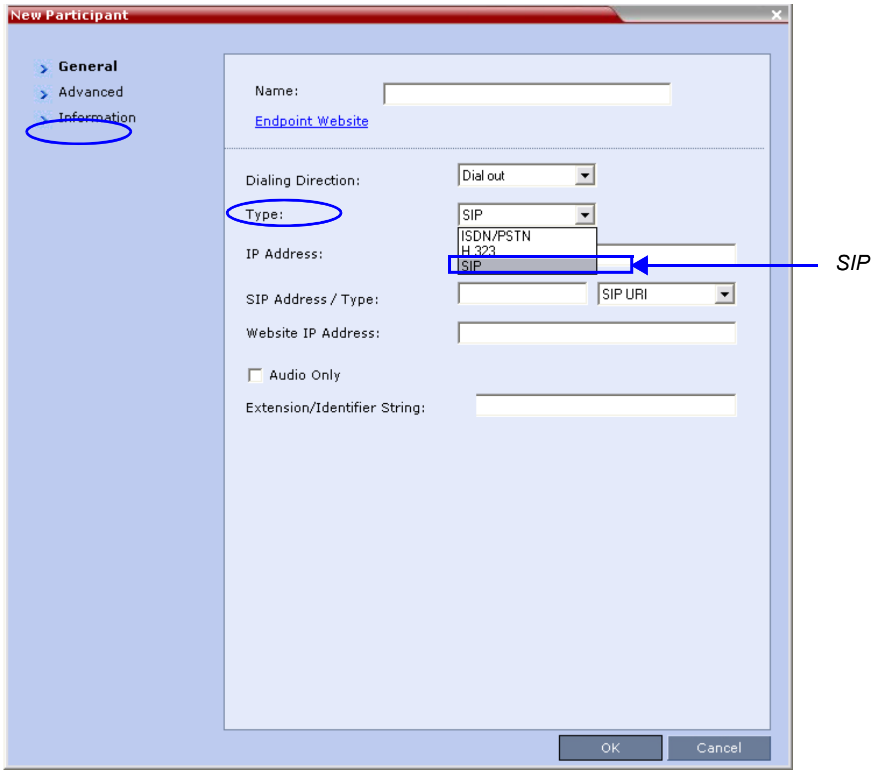
- *System Resource* usage is the same as for the *H.264* protocol. Table 3-5 summarizes *System Resource* usage for each of the supported resolutions.

Table 3-5 RTV - Resources by Resolution

Resolution	Video Resources Used
QCIF / CIF30	1
VGA (SD30) / W4CIF	1.5
HD720p30	3

Participant Settings

When defining a new participant or modifying an existing participant, select **SIP** as the participant's networking environment *Type* in the *New Participant* or *Participant Properties - General* tab.



The participants *Video Protocol* in the *New Participant* or *Participant Properties - Advanced* tab should be left at (or set to) its default value: **Auto**.

The **Auto** setting allows the video protocol to be negotiated according to the endpoint's capabilities:

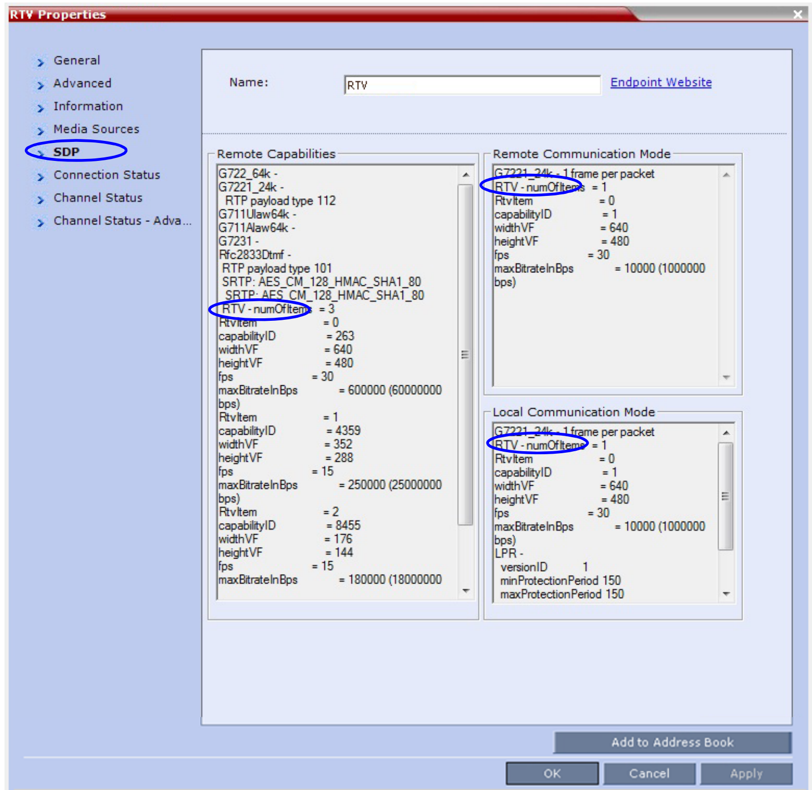
- *OCS* endpoints and *Lync Server* clients connect to the conference using the *RTV* protocol.
- Other endpoints negotiate the video protocol in the following sequence: *H.264*, followed by *RTV*, followed by *H.263* and finally *H.261*.

Protocol Forcing

Selecting *H.264*, *RTV*, *H.263* or *H.261* as the *Video Protocol* results in endpoints that do not support the selected *Video Protocol* connecting as *Secondary* (audio only).

Monitoring RTV

RTV information appears in all three panes of the *Participant Properties* - SDP tab.



Controlling Resource Allocations for Lync Clients Using RTV Video Protocol

The number of resources used by the system to connect a Lync client with RTV is determined according to the conference line rate and the Maximum video resolution set in the *Conference Profile*.

In versions 7.6 and earlier, when conferences are set to line rates above 600 kbps, the RMX could allocate up to three video resources to Lync clients connecting using the RTV video protocol.

From version 7.6.1, the system flag **MAX_RTV_RESOLUTION** enables you to override the RMX resolution selection and limit it to a lower resolution. Resource usage can then be minimized the 1 or 1.5 video resources per call instead of 3 resources, depending on the selected resolution.
Possible flag values are: **AUTO** (default), **QCIF**, **CIF**, **VGA** or **HD720**.

For example, if the flag is set to VGA, conference line rate is 1024Kbps, and the Profile Maximum Resolution is set to Auto, the system will limit the Lync RTV client to a resolution of VGA instead of HD720p and will consume only 1.5 video resources instead of 3 resources.

When set to **AUTO** (default), the system uses the default resolution matrix based on the conference line rate.

To change the default flag setting, add the MAX_RTV_RESOLUTION flag to the *System Configuration* flags and set its value. For information, see .

The following table summarizes the RMX resources allocated to a Lync Client based on the MAX_RTV_RESOLUTION flag setting, the connection line rate and the video resolution.

Table 3-6 *Selected video resolution based on flag setting and conference line rate and core processor*

Maximum Resolution Value	**Line Rate**	**Selected Video Resolution Per Core Processor**		
		Quad	**Dual**	**Single**
AUTO	> 600 kbps	HD720p 30fps	VGA 30fps	VGA 15fps
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
HD720p	> 600 kbps	HD720p 30fps	HD720p 13fps	VGA 15fps
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
VGA	> 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
CIF	> 600 kbps	CIF	CIF	CIF
	250 kbps - 600 kbps	CIF	CIF	CIF
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
QCIF	> 600 kbps	QCIF	QCIF	QCIF
	250 kbps - 600 kbps	QCIF	QCIF	QCIF
	180 kbps - 249 kbps	QCIF	QCIF	QCIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF

When the MAX_ALLOWED_RTV_HD_FRAME_RATE flag equals 0 (default value), Table 1-1 for the MAX_RTV_RESOLUTION flag applies. When the MAX_ALLOWED_RTV_HD_FRAME_RATE flag does not equal 0, see "*Threshold HD Flag Settings using the RTV Video Protocol"* on page **3-30** for more information.

The following table describes the number of allocated video resources for each video resolution when using the RTV protocol.

Table 3-7 *Allocated video resolutions per video resolution*

Selected Video Resolution	Number of Allocated Video Resources
HD720p	3
VGA	1.5
CIF	1
QCIF	1

Threshold HD Flag Settings using the RTV Video Protocol

The system flag **MAX_ALLOWED_RTV_HD_FRAME_RATE** defines the threshold Frame Rate (fps) in which RTV Video Protocol initiates HD resolutions.

Flag values are as follows:

- Default: **0** (fps) - Implements any Frame Rate based on Lync RTV Client capabilities

> If the MAX_RTV_RESOLUTION flag is set to AUTO dual core systems always view VGA. For more information on Lync RTV Client capabilities, see , "*Controlling Resource Allocations for Lync Clients Using RTV Video Protocol"* on page **3-27** for more information.

- Range: **0-30** (fps)

For example, when the flag is set to 15 and the Lync RTV Client declares HD 720P at 10fps, because the endpoint's frame rate (fps) of 10 is less than flag setting of 15, then the endpoint's video will open VGA and not HD.

In another example, when the flag is set to a frame rate of 10 and the Lync RTV Client declares HD 720P at 13fps, because the endpoint's frame rate (fps) of 13 is greater than flag setting of 10, then the endpoint's video will open HD and not VGA.

> - Single core PC's cannot view HD and always connect in VGA.
> - Dual Core Processor - The threshold for flag settings on Dual Core systems is 13 (fps) and less for viewing HD. When system flag is set to 14 (fps) or higher, the RTV Video Protocol shall connect in VGA.
> - Quad Core PC systems always view HD, even when flag settings are set anywhere from to 0-30.
> - The number of resources used by the system to connect a Lync client with RTV is determined according to the conference line rate and the maximum video resolution set in the Conference Profile. For more information, see "*Microsoft RTV Video Protocol Support in CP Conferences"* on page **3-24**.

4

Additional Conferencing Information

Various conferencing modes and video features require additional settings, such as system flag settings, conference parameters and other settings. In depth explanations of these additional settings are described in the following sections:

- "*H.239 / People+Content*" on page **4-2**
- "*Video Preview*" on page **4-26**
- "*Gathering Phase*" on page **4-30**
- "*Audio Algorithm Support*" on page **4-35**
- "*Media Encryption (AVC Only)*" on page **4-40**
- "*Packet Loss Compensation (LPR and DBA)*" on page **4-50**
- "*Telepresence Mode (AVC Only)*" on page **4-55**
- "*Lecture Mode (AVC Only)*" on page **4-73**
- "*Permanent Conference*" on page **4-80**
- "*Audio Algorithm Support*" on page **4-35**

MPM+ and MPMx cards support additional video resolutions and video quality enhancement such as Video Clarity™ in addition to all video modes and features supported by MPM cards.

MPMx card offers additional functionality, such as support of H.264 High Profile, enhanced display of *Site Names* and *Message Overlay* and more.

- The RealPresence Collaboration Server (RMX) 1500 contains only one MPMx card.
- The RealPresence Collaboration Server (RMX) 2000 can function with three types of video Media Processing Modules (MPM): MPM, MPM+ and MPMx. These cards differ in their port capacity and their support of video resolutions.

From *Version 7.1*, *MPM* media cards are not supported.

- The RealPresence Collaboration Server (RMX) 4000 can contain MPM+ or MPMx cards.

H.239 / People+Content

H.239

The *H.239* protocol allows compliant endpoints to transmit and receive two simultaneous video streams:

- **People video stream** – video is displayed in Continuous Presence or Video Switching conferencing mode or in Media Relay (SVC) conferencing Mode
- **Content video stream** – Video Switching mode for content sharing

By default, all conferences, *Entry Queue*s, and *Meeting Rooms* launched on the *RMX* have *H.239* capabilities.

To view *Content*, endpoints must use the same Bit Rate, Protocol, and Resolution. An AVC endpoint may not send *Content* while connecting to an *Entry Queue*.

Endpoints without *H.239* capability can connect to the video conference without *Content*.

Cascade links declare *H.239* capabilities and they are supported in *Star* and *MIH* cascading topologies. For more details, see "*Cascading Conferences - H.239-enabled MIH Topology"* on page **5-26**.

People+Content

People+Content utilizes a different signaling protocol and is *Polycom's* proprietary equivalent of *H.239*.

Guidelines

- All network environments are supported.
- Conferences can include a mix of endpoints that support *H.239* or *People+Content*.
- All endpoints will receive Content at the highest resolution common to all connected endpoints.
- *SIP People+Content* is supported with *MPM+* and *MPMx* cards.
- *H.239* is supported in *MIH*, *Star* and *Basic Cascading* topologies.
- *People+Content* is supported in cascaded conferences but cannot be used as the protocol for a cascade link.
- If an endpoint supports both *H.239* and *People+Content* protocols, *H.239* is selected as the preferred communications protocol.
- *H.263 Annex T* and *H.264* protocols are supported for *Content* transmission.
- *People+Content* is enabled by default. It can be disabled for all conferences and endpoints by manually adding the **ENABLE_EPC** *System Flag* to the *System Configuration* and setting its value to **NO** (default setting is **YES**).
- Endpoints that support *People+Content* (for example, *FX* endpoints) may require a different signaling protocol. For these endpoints, manually add the *System Flag* **CS_ENABLE_EPC** to the *System Configuration* and set its value to **YES** (default value is **NO**).
- Content sharing is not supported in Microsoft ICE environment (BFCP protocol).

- Video endpoints that do not support SIP Content (such as PVX), can receive Content on the People channel if the conference is set to *Send Content to Legacy Endpoints*. For more details see, "*Sending Content to Legacy Endpoints (AVC Only)"* on page **4-17**.

SIP BFCP Content Capabilities

SIP Clients supporting *BFCP* over *UDP,* when connected to conferences on the RMX, can share *Content* with endpoints supporting the following *Content* sharing protocols:

- *BFCP/TCP*
- *BFCP/UDP*
- *H.323/ H.239*
- *H.323 /Polycom People+Content*
- *ISDN Content*

Guidelines:

For *SIP Clients* that support both *BFCP/TCP* and *BFCP/UDP*:

- The preferred protocol is *BFCP/UDP*.
- When used in *Cascading* conferences, the *Cascade Link* must be *H.323*.
- *BFCP/UDP* is supported in both *IPv4* and *IPv6* addressing modes.
- *BFCP* utilizes an unsecured channel (port 60002/TCP) even when *SIP TLS* is enabled. If security is of higher priority than *SIP* content sharing, *SIP People+Content* can be disabled. To do this manually add the **ENABLE_SIP_PEOPLE_ PLUS_CONTENT** *System Flag* to the *System Configuration* and set its value to **NO**.
- *SIP People+Content* and *BFCP* capabilities are by default declared to all endpoints. If, however, the endpoint identity is hidden by a proxy server, these capabilities will not be declared by the RMX. Capabilities declaration is controlled by the **ENABLE_SIP_PPC_FOR_ALL_USER_AGENT** *System Flag*.

  The default value of the **ENABLE_SIP_PPC_FOR_ALL_USER_AGENT** *System Flag* is **YES** resulting in *BFCP* capability being declared with all vendors' endpoints unless it is set to **NO**. When set to **NO**, the RMX will declare *SIP People+Content* and *BFCP* capabilities to *Polycom* and *Avaya* endpoints.
- The **CFG_KEY_ENABLE_FLOW_CONTROL_REINVITE** *System Flag* should be set to **NO** when *SIP BFCP* is enabled.
- If these *System Flags* don't exist in the system, they must be manually added. For more information see "*Modifying System Flags"* on page **22-1**.
- BFCP capabilities are not supported in Microsoft ICE environment.

Dial-out Connections:

- For dial-out connections to *SIP Clients*, *BFCP/UDP* protocol can be given priority by adding the adding the **SIP_BFCP_DIAL_OUT_MODE** *System Flag* to *system.cfg* and setting its value to UDP.

The *RMX' s Content* sharing determined by the *System Flag's* settings and *SIP Client* capabilities are summarized in Table 4-1.

Table 4-1 *System Flag - SIP_BFCP_DIAL_OUT_MODE*

<table>
<tr><th rowspan="2">Flag Value</th><th colspan="3">SIP Client: BFCP Support</th></tr>
<tr><th>UDP</th><th>TCP</th><th>UDP and TCP</th></tr>
<tr><td>AUTO (Default)</td><td rowspan="2">BFCP/UDP selected as Content sharing protocol.</td><td>BFCP/TCP selected as Content sharing protocol.</td><td rowspan="2">BFCP/UDP selected as Content sharing protocol.</td></tr>
<tr><td>UDP</td><td>Cannot share Content.</td></tr>
<tr><td>TCP</td><td>Cannot share Content.</td><td colspan="2">BFCP/TCP selected as Content sharing protocol.</td></tr>
</table>

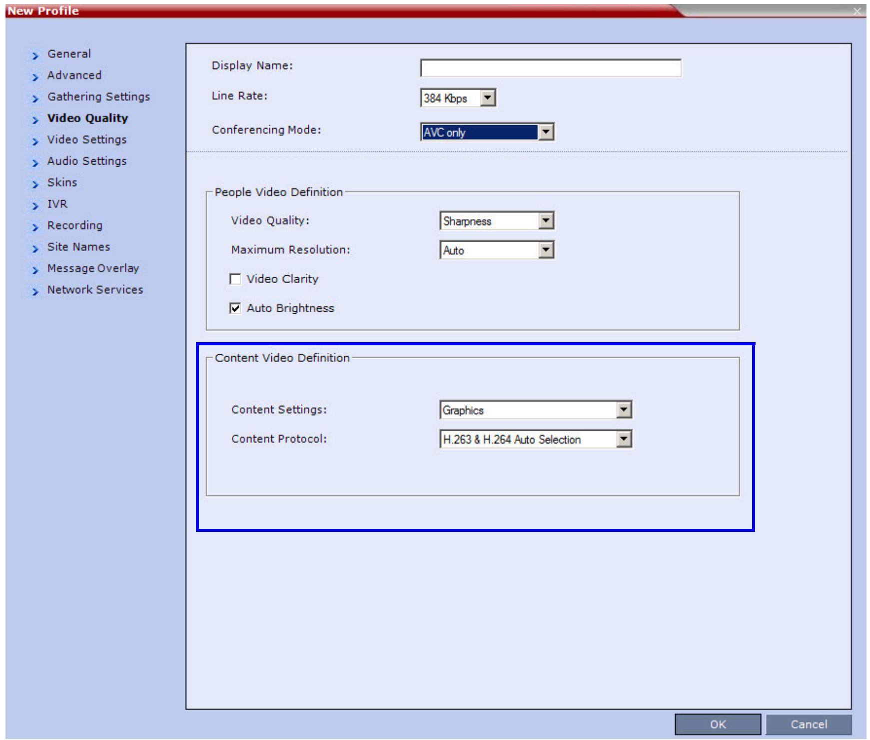
For more information see "*Manually Adding and Deleting System Flags"* on page **22-18**.

Dial-in Connections:

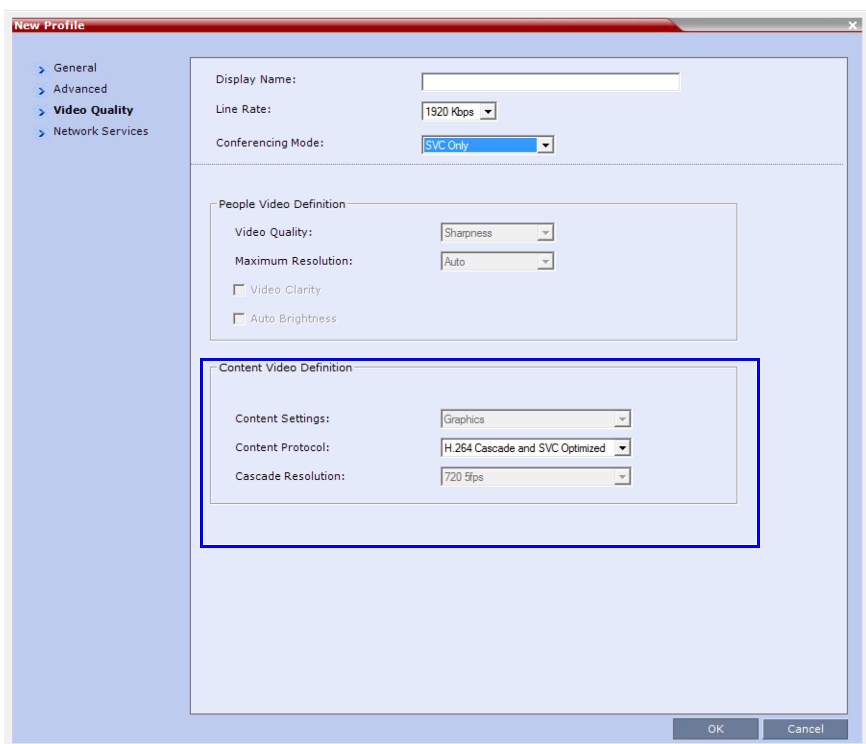
- The RMX will share content with *Dial-in SIP Clients* according to their preferred *BFCP* protocol.
- *SIP Clients* connected as *Audio Only* cannot share *Content*.

Defining Content Sharing Parameters for a Conference

Content parameters are defined in the *Conference Profiles - Video Quality* dialog box. The parameters change according to the *Conferencing Mode*.



AVC Conferencing Mode



SVC Conferencing Mode

1 In the *Content Video Definition* section, select the *Content Settings* and *Protocol* as follows:

Table 4-2 *H.239 Content Options*

Field	Description
Content Settings	Select the transmission mode for the Content channel: • ***Graphics*** — basic mode, intended for normal graphics • ***Hi-res Graphics*** (AVC Only) — a higher bit rate intended for high resolution graphic display • ***Live Video*** (AVC Only) — Content channel displays live video • ***Customized Content Rate*** (AVC Only) **-** manual definition of the Conference Content Rate**,** mainly for cascading conferences. Selection of a higher bit rate for the *Content* results in a lower bit rate for the people channel. For a detailed description of each of these options, see "*Content Settings"* on page **4-7**.

Content Protocol	• **H.263** (AVC Only)
	  • *Content* is shared using the *H.263* protocol.
	  • Use this option when most of the endpoints support *H.263* and some endpoints support *H.264*.
	• **H.263 & H.264 Auto Selection** (AVC Only Default)
	  • *Content* is shared using *H.263* if a mix of H.263-supporting and *H.264*-supporting endpoints are connected.
	  • *Content* is shared using *H.264* if all connected endpoints have *H.264* capability.
	• **H.264 HD** (AVC Only)
	  • Ensures high quality *Content* when most endpoints support *H.264* and *HD Resolutions*.
	• **H.264 Cascade and SVC Optimized**
	  • All *Content* is shared using the *H.264* content protocol and is optimized for use in *SVC only* and *Cascaded Conferences*.
	For a detailed description of each of these settings, see "*Content Protocols"* on page **4-8**..

Cascade Resolution	Select a *Cascade Resolution* from the drop-down menu. The *Cascade Resolutions* that are available for selection are dependent on the *Line Rate* and *Content Settings* that have been selected for the conference. For a full list of *Cascade Resolutions* see "*Bit Rate Allocation to Content Channel by Line Rate, Content Settings & Cascade Resolution in AVC Conferencing"* on page **4-12**. **Note:** This field is only displayed when *H.264 Cascade and SVC Optimized* is selected as the *Content Protocol* and is enabled for selection in AVC Only conferences. This option is disabled in SVC conferences.

2 Click **OK.**

Content Settings

The Content channel can transmit one of the following modes:

- **Graphics** – for standard graphics. This is the default mode in AVC conferences and the only supported mode for SVC conferences.
- **Hi-res Graphics** (AVC only conferences) – requiring a higher bit rate, for high quality display or highly detailed graphics.
- **Live Video** (AVC only conferences) – highest bit rate, for video clips or live video display.
- **Customized Content Rate** (AVC only conferences) - that allows manual definition of the *Conference Content Rate*.

AVC Only Content Setting

For *Graphics*, *Hi-res Graphics* and *Live Video*, the highest common Content bit rate is calculated for the conference each time an endpoint connects. Therefore, if an endpoint connects to an ongoing conference at a lower bit rate than the current bit rate, the Content bit rate for the current conference is re-calculated and decreased.

Bit rate allocation by the MCU is dynamic during the conference and when the Content channel closes, the video bit rate of the *People conference* is restored to its maximum.

During a conference the MCU will not permit an endpoint to increase its bit rate, it can however change its Content resolution. The RMX can decrease the allocated Content bit rate during a conference.

Table 4-3 summarizes the bit rate allocated to the Content channel from the video channel in each of the *Content Settings* according to the conference line rate:

Table 4-3 Decision Matrix - Bit Rate Allocation to Content Channel per Conference Line Rate

Content Settings	Content Bit Rate Allocation per Conference Line Rate (kbps)											
	64 96	**128**	**256**	**384**	**512**	**768 832**	**1024 1152**	**1472 1728**	**1920**	**2048**	**4096**	**6144**
Graphics		64	64	128	128	256	256	256	256	256	256	1536
Hi Resolution Graphics		64	128	192	256	384	384	512	768	768	1536	1536
Live Video		64	128	256	384	512	768	768	1152	1152	1536	1536
Customized Content Rate	The Content Bit Rate is selected from a menu in the *Content Video Definition* pane. See "*Selecting a Customized Content Rate in AVC Conferences"* on page 4-14.											

Table 4-4 summarizes the *Maximum Resolution* of *Content* and *Frames per Second (fps)* for *Bit Rate Allocations* to the *Content Channel* as set out in *Table 4-3*.

Table 4-4 *Content - Maximum Resolution, Frames/Second per Bit Rate Allocation*

Bit Rate Allocated to Content Channel (Kbps)	Content	
	Maximum Resolution	**Frames/Second**
*From **64** and less than **512***	H.264 HD720p	5
*From **512** and less than **768***	H.264 HD720p	30
*From **768** and up to **1536***	H.264 HD1080p	15

SVC Only Content Setting

The Content channel is transmitted in **Graphics** mode only.

Content Protocols

Two *Content Protocols* can be used for sharing content:

- H.263 (AVC only)
- H.264 (AVC and SVC conferences)

H.264 offers higher quality content, but is not supported by legacy endpoints. Depending on the endpoints capabilities, you can determine the content sharing experience by selecting the appropriate protocol and system behavior from the *Content Protocol* list:

- *H.263 & H.264 Auto Selection* (AVC only)
- *H.263* (AVC only)
- *H.264 HD* (AVC only)
- *H.264 Cascade and SVC Optimized* (AVC and SVC conferences)

H.263 & H.264 Auto Selection (AVC Default Setting)

The **H.263 & H.264 Auto Selection** option should be selected when *Content* is to be shared using a mix of *H.263*-supporting and *H.264*-supporting endpoints. (In versions up to and including 7.6, this is named ***Up to H.264***.)

Bit rate allocation to the *Content* channel by the RMX is dynamic according to the conference line rate and *Content Setting* selected for the conference.

If an endpoint that supports only *H.263* for Content Sharing connects to a conference with Content Protocol set to *H.263 & H.264 Auto Selection*:

- *Content* is shared using *H.263* even if *H.264*-supporting endpoints are connected.
- *Content* is shared using *H.264* if all connected endpoints have *H.264* capability.
- If the first endpoint to connect to the conference only supports *H.263,* the *H.263* protocol is used for *Content* for all conference participants.
- If *Content* is already being shared using the *H.264* protocol when a *H.263* endpoint connects, *Content* sharing is stopped and must be manually restarted using *H.263* (i.e. the endpoint using H.263 Content Protocol must connect first), for all participants to receive content. If the *H.263* endpoint disconnects, *Content* sharing must be manually stopped and restarted and will automatically upgrade to the *H.264* protocol.

- Endpoints that do not have at least *H.263* capability can connect to the conference but cannot share *Content*.
- This option is not available in *SVC Conferencing Mode*.

H.263 (AVC Only Conferences)

Select this option when most of the endpoints support *H.263* and some endpoints support *H.264*. In such a case, all endpoints will share content using the H.263 protocol, and this protocol will not change throughout the conference (fix mode).

Bit rate allocation to the *Content* channel by the RMX is dynamic according to the conference line rate and *Content Settings* selected for the conference. For more information see "*Content Settings"* on page **4-7**.

This option is not available in *SVC Conferencing Mode*.

H.264 HD (AVC Only Conferences)

The **H.264 HD** option should be selected only if most endpoints in the conference support *H.264* to ensure high quality *Content*.

When this protocol option is selected, endpoints must connect at *Content* bit rates above a minimum as specified by specific *System Flags* to ensure high quality *Content* for all participants. For more information about *System Flags* see "*Setting the Minimum Content Rate for Each Content Quality Setting for H.264 HD"* on page **4-9**.

Bit rate allocation to the *Content* channel by the RMX is dynamic according to the conference line rate and *Content Setting* selected for the conference. For more information see "*Content Settings"* on page **4-7**.

Endpoints that do not support *H.264*, or these that do not meet the minimum line rate threshold for the *Content Setting* along with *ISDN* endpoints, are connected as *Legacy Endpoints* and receive content through their video channel. If the *Send Content to Legacy Endpoints* selection is disabled these endpoints will not receive content.

Guidelines

- Only endpoints that support *H.264* capability at a resolutions of *HD720p5* or higher will be able to receive and send *Content*.
- This option is not available in *SVC Conferencing Mode*.
- When *H.264 HD* is selected, the *Send Content to Legacy Endpoints* selection is enabled by default in the *Conference Profile – Video Settings* tab.
- In *MPM+ Card Configuration Mode*, maximum supported content resolution is HD 720p.
- Once an endpoint is categorized as a *Legacy Endpoint* and receives the content over the video channel, it remains in this mode without the ability to upgrade to H.264 HD content and receive content over the Content channel.
- The minimum *Content Rate* required for allowing a participant to share *Content* is the lower valued parameter when comparing the *System Flag* setting *(*Table 4-5*)* and the *content bit rate allocation* derived from the conference line rate (Table 4-3*)*.

  When the flag settings enable an endpoint to share Content at a content rate that is lower than the conference content rate (Table 4-3), the content rate of the entire conference is reduced to the content rate supported by that endpoint.

Setting the Minimum Content Rate for Each Content Quality Setting for H.264 HD

The following *System Flags* determine the minimum content rate required for endpoints to share *H.264* high quality content via the *Content* channel.

A *System Flag* determines the minimum line rate for each *Content Setting*:

- *Graphics*
- *Hi Resolution Graphics*
- *Live Video*

In order to change the *System Flag* values, the flags must be manually added to the *System Configuration*. For more information see "*Modifying System Flags"* on page **22-1**.

Table 4-5 *H.264 HD System Flags*

Content Settings	Flag Name	Range	Default
Graphics	*H264_HD_GRAPHICS_MIN_CONTENT_RATE*	0-1536	128
Hi Resolution Graphics	*H264_HD_HIGHRES_MIN_CONTENT_RATE*	0-1536	256
Live Video	*H264_HD_LIVEVIDEO_MIN_CONTENT_RATE*	0-1536	384

Example

Table 4-6 summarizes an example of two participants trying to connect to a conference running at a *Line Rate* of 1024Kbps. The *Content Setting* for the conference is **Hi Resolution Graphics** and the **H264_HD_HIGHRES_MIN_CONTENT_RATE** *System Flag* setting are used to determine if *Content* will be shared with the participant.

Table 4-6 *Participant Content Sharing Based on cOnnection Line Rate and System Flag Setting*

<table>
<tr><th rowspan="2"></th><th colspan="2">Participant</th><th colspan="2">Conference</th><th rowspan="2">Flag Value</th><th rowspan="2">Result</th></tr>
<tr><th>Line Rate</th><th>Bit Rate Allocation to Content Channel (Table 4-3)</th><th>Line Rate</th><th>Bit Rate Allocation to Content Channel (Table 4-3)</th></tr>
<tr><td rowspan="2">Participant 1</td><td rowspan="2">384</td><td rowspan="2">192</td><td rowspan="4">1024</td><td rowspan="4">384</td><td>128</td><td>Participant and entire conference share content at 192Kbps</td></tr>
<tr><td>512</td><td>Participant receives content in the video channel (Legacy)</td></tr>
<tr><td rowspan="2">Participant 2</td><td rowspan="2">1024</td><td rowspan="2">384</td><td>128</td><td>Participant and entire conference share content at 384Kbps</td></tr>
<tr><td>512</td><td>Participant and entire conference share content at 384Kbps</td></tr>
</table>

H.264 Cascade and SVC Optimized

The **H.264 Cascade and SVC Optimized** option maintains content quality and minimizes the amount of content refreshes that occur in large cascading conferences when participants connect or disconnect from the conference.

This option is the only available option automatically selected in SVC Only conferences .

The *H.264 Cascade and SVC Optimized* option uses fixed resolution and frame rate for SVC Only conferences. In AVC conferences, each content *Line Rate* and *Content Setting* has its own resolution and frame rate as summarized in Table 4-7.

In AVC conferences, endpoints that do not support the required content parameters (*Content* line rate, *H.264* protocol and *Content Resolution)*, along with *ISDN* endpoints, can be connected as *Legacy Endpoints* and receive content through their video channel. This ensures that *Content* settings are not changed following the participants connection or disconnection from the conference. If the *Send Content to Legacy Endpoints* option is disabled, these endpoints will not receive content.

In SVC Only conferences, endpoints that do not support the required content parameters (*Content* line rate and *Content Resolution)* cannot share content.

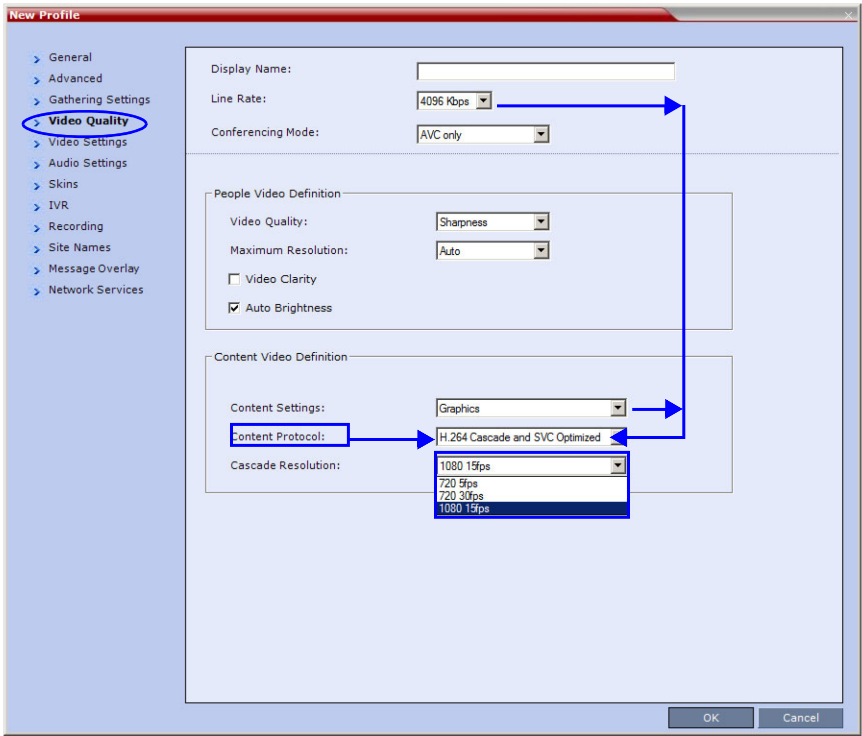
Guidelines

- In Cascading conferences, the cascade link must be *H.323.*
- This is the only available Content sharing mode in *SVC Conferencing Mode*.
- *H.323*, *SIP* and *ISDN* participants are supported in *AVC Conferencing Mode*.
- *H.264 High Profile* is not supported.
- In *MPM+ Card Configuration Mode*, maximum supported content resolution is HD 720p.
- When *H.264 Cascade and SVC Optimized* is selected in AVC Conferencing Mode, the *Send Content to Legacy Endpoints* selection is enabled by default in the *Conference Profile – Video Settings* dialog box.
- In *AVC Conferencing Mod*e, endpoints that cannot connect at a line rate required to support the conference Content Rate are considered *Legacy Endpoints* and will receive Content in the video channel.
- In *SVC Conferencing Mod*e, endpoints that cannot connect at a line rate required to support the conference Content Rate will receive Content in the video channel.

Enabling H.264 Cascade and SVC Optimized Content Sharing in AVC Conferences

When *H.264 Cascade and SVC Optimized* is selected in **AVC** conference as the *Content Protocol*, an additional field, *Cascade Resolution* is displayed in the *Content Video Definition* pane. In *SVC Conferencing Mode,* the *Cascade Resolution* option is disabled.

The *Cascade Resolution* is a fixed resolution and frame rate for *Content* sharing in a Cascaded Conference. The *Cascade Resolutions* that are available for selection are dependent on the *Line Rate* and *Content Settings* that have been selected for the conference.



AVC Conferencing Mode

Table 4-7 summarizes the interaction of these parameters.

Table 4-7 *Bit Rate Allocation to Content Channel by Line Rate, Content Settings & Cascade Resolution in AVC Conferencing*

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Graphics	HD720/5		64	128	128	256	256	256	512	512
	HD720/30							512	512	512
	HD1080/15						768	768	1152	1152
Hi Resolution Graphics	HD720/5			192	256	384	384	512	768	512
	HD720/30							512	768	768
	HD1080/15								768	1152

***Table 4-7** Bit Rate Allocation to Content Channel by Line Rate, Content Settings & Cascade Resolution in AVC Conferencing (Continued)*

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Live Video	HD720/5			256	384	512	768	768	768	768
	HD720/30					512	768	768	768	768
	HD1080/15						768	768	1152	1152

The selection of the appropriate *Content Resolution* option, when several options are available, should be based on the line rate and capabilities that can be used by most or all endpoints connecting to the conference.

Examples:

- If the conference *Line Rate* is **1024** kbps.

  and

- If the *Content Settings* selection is **Graphics**.
  - **Cascade Resolutions** of **HD720/5** and **HD1080/15** are selectable with **256** kbps and **768** kbps allocated as the *Conference Content Rate* respectively.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Graphics	HD720/5		64	128	128	256	**256**	256	512	512
	HD720/30							512	512	512
	HD1080/15						**768**	768	1152	1152

The higher *Cascade Resolution,* **HD1080/15** should be selected only if most of the endpoints connecting to the conference can support a *Content Rate* of 768Kbps, which requires the participant to connect to the conference at a *Line Rate* of 1024kbps.

When the lower *Cascade Resolution* **HD720/5** is selected, the conference *Content Rate* is set to 256 kbps. This will enable the endpoints that connect to the conference at a *Line Rate* of at least 768 kbps to receive content in the Content channel. Endpoints that connect to the conference at a line rate lower than 768Kbps, will receive content in the video channel.

- If the *Content Settings* selection is **Hi Resolution Graphics**.
  — Only **HD720/5** can be selected as the *Cascade Resolution* with **384** kbps allocated as the conference *Content Rate*.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Hi Resolution Graphics	HD720/5			192	256	384	384	512	768	512
	HD720/30							512	768	768
	HD1080/15								768	1152

Only endpoints that connect at a *Line Rate* of 1024 kbps that is required to support a *Content Rate* of 384 kbps will receive content in the Content channel. Endpoints that connect to the conference at a line rate lower than 1024 kbps, will receive content in the video channel.

- If the *Content Settings* selection is **Live Video**.
  — **HD720/5**, **HD720/30** or **HD1080/15** can be selected as the *Cascade Resolution* with **768** kbps allocated the as the *Conference Content Rate.*

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)								
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144
Live Video	HD720/5			256	384	512	768	768	768	768
	HD720/30					512	768	768	768	768
	HD1080/15						768	768	1152	1152

The higher *Cascade Resolution* should be selected according to the resolution capabilities of the majority of the endpoints connecting to the conference. Endpoints that cannot support the selected *Cascade Resolution* are considered *Legacy Endpoints* and will receive *Content* in the video channel.

Selecting a Customized Content Rate in AVC Conferences

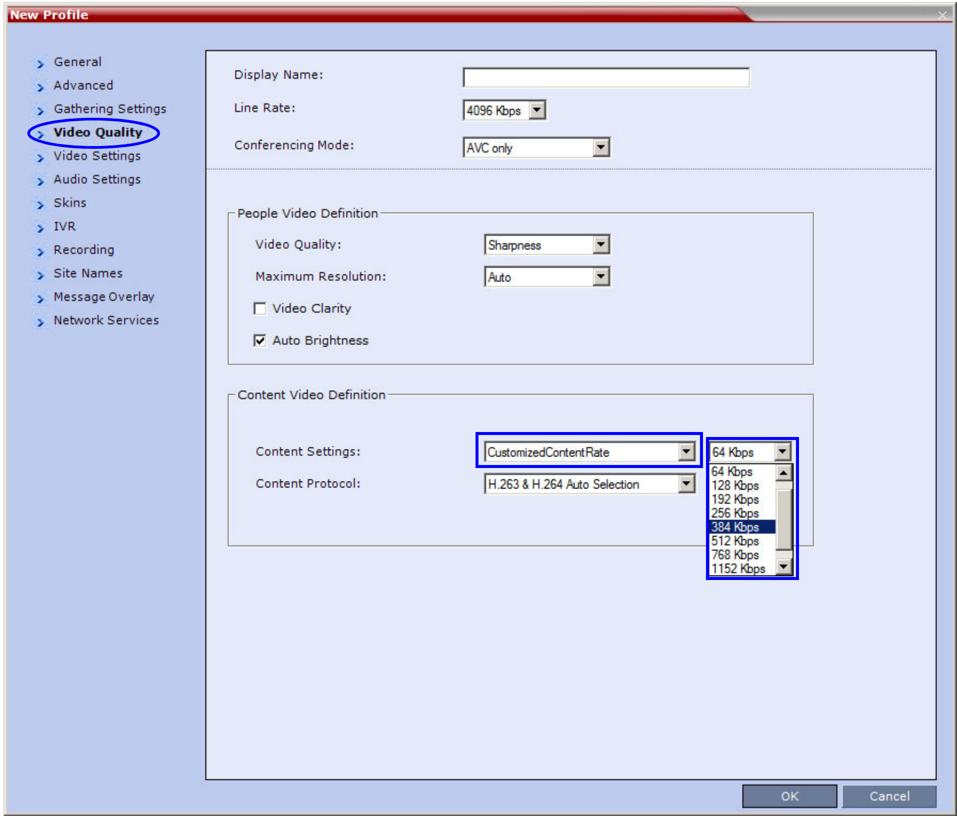
Customized Content Rate functionality can be implemented when a *Conference Content Rate*, that is automatically calculated by the *RMX*, may not be suitable in a *Cascaded Environment*, where conference line rates may vary widely between the cascaded conferences. For example, one conference may have a line rate of 4 Mbps, and the other a line rate of is 512kbps.

Guidelines:

- Cascaded conferences may have different *Conference Line Rates*.
- The *Customized Content Rate* must be the same for all cascaded conferences.

To Select the Customized Content Rate:

Customized Content Rate is enabled in the *Profile - Video Quality* dialog box.



1 In the Content Settings list, select **Customized Content Rate**.
When selected, a drop-down menu of the available *Conference Content Rates* is displayed. These *Content Line Rates* are based on and will vary according to the selected *Conference Line Rate*.

The largest selectable *Content Line Rate* is 66% of the *Conference Line Rate*.

If the *Conference Line Rate* is 64kbps or 96kbps, the only available *Conference Content Rate* is **0**, indicating that *Content* is not supported at these rates.

2 Select the required content rate.

When selecting a *Conference Line Rate* (after selecting *Customized Content Rate)* that is too low to support the selected *Customized Content Rate*, the following error message is displayed:
"The selected content line rate should be modified. To update content line rate press Cancel. To return to automatic mode (Graphics) press OK."

You can then modify either the *Content Line Rate* or the *Conference Line Rate* or select another *Content Setting* option.

3 If **H.264 Cascade and SVC Optimized** is the selected *Content Protocol*, a **Cascade Resolution** must be selected.

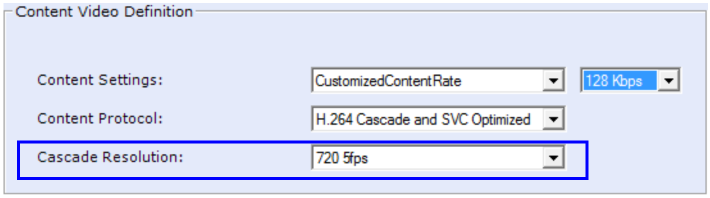


Table 4-8 lists the *Cascade Resolutions* available for the various *Conference Content Rates*.

Table 4-8 *H.264 Cascade Optimized - Cascade Resolutions*

H.264 Cascade Optimized			
Conference Content Rate (Kbps)	**Available Resolutions***		
64	HD720p5 Content Not Supported		
128	HD720p5		
192	HD720p5		
256	HD720p5		
384	HD720p5		
512	HD720p5	HD720p30	
768	HD720p5	HD720p30	HD1080p15
1152	HD720p5	HD720p30	HD1080p15
1536	HD720p5	HD720p30	HD1080p15

*The default resolution for all *Content Rates* is *HD720p5*.

Modifying the Threshold Line Rate for HD Resolution Content

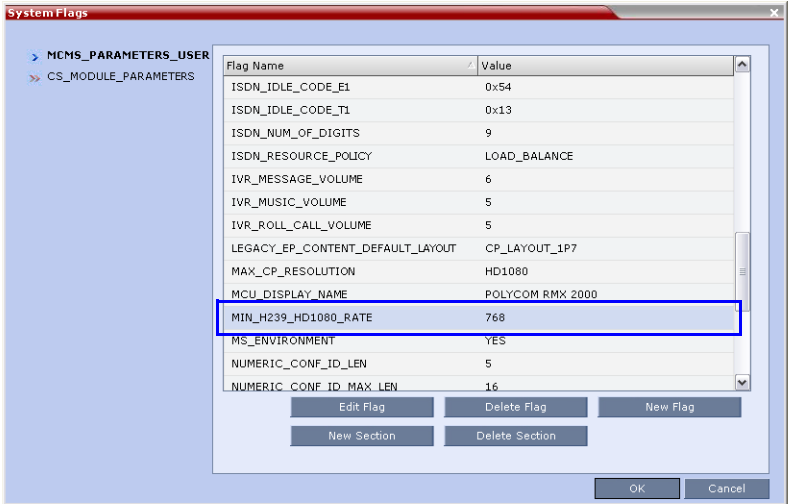
The threshold line rate for *HD Resolution Content* is the line rate at which the RMX will send *Content* at *HD1080 Resolution*. The default is 768 kbps. When the threshold value is set to 0, HD720p/ HD1080p resolutions for Content sharing are disabled.

To modify the HD Resolution Content threshold line rate:

1 On the RMX menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.

2 In the *MCMS_PARAMETERS* tab, double-click the **MIN_H239_HD1080_RATE** entry.



The *Update Flag* dialog box is displayed.

3 In the *Value* field, enter the minimum line rate at which *HD1080 Resolution Content* will be enabled.

— Enter **0** to disable this flag and prevent HD Content from being used.

4 Click **OK** to confirm and exit the *Update Flag* dialog box**.**

5 Click **Close** to exit the *System Flags* dialog box.

Sending Content to Legacy Endpoints (AVC Only)

The RMX can be configured to send *Content* to *H.323/SIP/ISDN* endpoints that do not support *H.239 Content* (legacy endpoints) over the video (people) channel, allowing the participants using legacy endpoints to view *Content* instead of the other conference participants.

Guidelines for Sending Content to Legacy Endpoints

- This option is enabled in *MPM+* and *MPMx Card Configuration Modes* only.
- This option is valid when sending Content as a separate stream is enabled in the *System Configuration* and the flag: ENABLE_H239 is set to YES.
- An Additional video resource is allocated to the conference when Content is sent to legacy endpoints:
  — In *MPM+* mode, one *SD* video resource.
  — In *MPMx* mode, one *HD* video resource.

  The allocation is done only when a legacy endpoint is connected to the conference and a Content session is initiated and transmitted via the video channel. Once the resource is allocated, it remains allocated to the conference until the conference ends.

  If the system cannot allocate the resource required for sending the Content, the conference status changes to “Content Resource Deficiency” and Content will not be sent to the legacy endpoints.

As the resource required for sending Content to legacy endpoints is allocated on the fly, when scheduling a reservation, in rare occasions when the MCU is fully loaded, “Resource deficiency” may be encountered. This may prevent participants from connecting to the conference or from Content being sent to the legacy endpoint. To ensure resource for sending Content to legacy endpoints, add one resource to the number of resources defined in the *Reserve Resources for Video Participants* field, in the *Conference Properties - General* dialog box.

- Non-H.239 (legacy) endpoints receive the Content via the video channel using the same video protocol and resolution with which they receive video.
- The highest Content resolution for legacy endpoints is:
  - *HD720p30* with *MPMx*
  - *HD720p5/6* with *MPM+*
- Once an endpoint is categorized as a *Legacy Endpoint* and receives the content over the video channel, it remains in this mode without the ability to receive content over the Content channel.
- Content cannot be sent to legacy endpoints when *Same Layout* mode is selected for the conference.
- This option in not supported in *Video Switching* conferences.
- When Content is transmitted, the Site Name of the endpoints cannot be viewed.
- Content can be sent to legacy endpoints in gateway calls.
- When moving a legacy participant to the *Operator conference*, Content will not be available to the legacy endpoint.
- An *FX* endpoint dialing in to an RMX with *MPMx* cards will receive content using *People + Content*. An *FX* endpoint dialed out from an RMX with *MPMx* cards will only receive content via the video channel using *People + Content* if *Send Content to Legacy Endpoints* is enabled in the *Conference Profile*.

Content Display on Legacy Endpoints

When Contents is sent to legacy endpoints, their video layout automatically changes to a “Content layout” which is defined by the system flag LEGACY_EP_CONTENT_DEFAULT_LAYOUT and the Content is shown in the larger/top left (“speaker”) window. The video layouts of the other conference participants do not change.

The switch to the Content layout occurs in the *Auto Layout*, *Presentation Mode*, *Lecture Mode* and when a layout is selected for the conference. However, in *Lecture Mode*, when Content is sent to legacy endpoints, when switching to the Content layout, the Content is shown in the “lecturer/speaker” window and the lecturer is show in a second window. If the layout contains more than two windows, all other windows will be empty. All other participants will see the lecturer in full screen.

In *Same Layout* mode, Content cannot be sent to legacy endpoints.

The LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag default is set to a layout of 1+4 where the Content is shown in the large window and the other conference participants are shown in the small windows. This default value can be changed in the *System Configuration*.

When Content is stopped, the layout of the legacy participants returns to the last video layout seen prior to the Content mode.

The Legacy participants can change their layout using *Click&View*. In such a case, the Content is forced to the “speaker” window.

The RMX user can also change the layout for the participants the legacy endpoints (selecting personal layout).

When forcing a video participant to the Content window (instead of Content), the Content display can be restored only by selecting any other video layout.

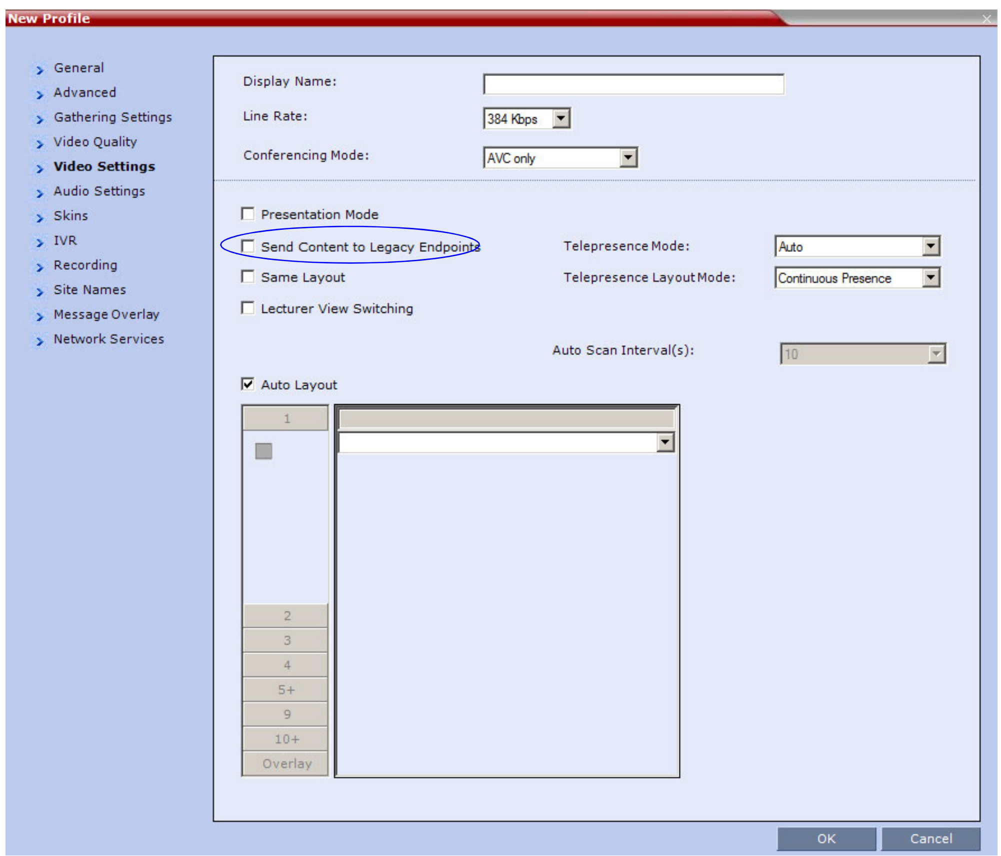
Interoperability with Polycom CMA and DMA

The CMA uses the Profiles that are stored in the RMX. If the *Send Content to Legacy Endpoints* option is enabled in the Conference Profile, this option will be enabled in the conference started from the CMA that uses that Profile. However, the CMA does not display an indication that this option is enabled for the conference.

A new conference can be started on the DMA using a Conference Profile that is defined on the RMX or by defining all the conference parameters. The *Send Content to Legacy Endpoints* option can be enabled only in the Conference Profile defined in the RMX, therefore, to include this option in the conference started on the DMA use an RMX existing Profile. However, the DMA does not display an indication that this option is enabled for the conference.

Enabling the Send Content to Legacy Endpoints Option

The **Send Content to Legacy Endpoint** option is enabled in the *Conference Profile - Video Settings* tab.



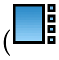
If the *Video Switching* option is selected in the *Conference Profile - General* tab, the *Send Content to Legacy Endpoints* option is disabled.

If the *Same Layout* option is selected in the *Conference Profile - Video Settings* tab, the *Send Content to Legacy Endpoints* option is disabled.

Note: Select this option when Avaya IP Softphone will be connecting to the conference.

Changing the Default Layout for Displaying Content on Legacy Endpoints

The default layout that will be used to display Content on the screens of legacy endpoints is defined by the system flag **LEGACY_EP_CONTENT_DEFAULT_LAYOUT.**

The configured default layout is 1+4 ( CP_LAYOUT_1P4VER). You can change the default layout configuration by entering a new value for the flag in the system configuration.

To modify system flags:

1 On the *RMX* menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.

2 In the *MCMS_PARAMETERS* tab, double-click the **LEGACY_EP_CONTENT_DEFAULT_LAYOUT** entry.
The *Edit Flag* dialog box is displayed.

3 In the *Value* field, enter the flag value for the required layout as follows:

Table 4-9 LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values

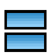
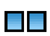
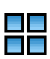
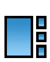
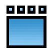
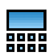
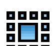
Layout	Flag Value
	CP_LAYOUT_1X1
	CP_LAYOUT_1X2
	CP_LAYOUT_1X2HOR
	CP_LAYOUT_1X2VER
	CP_LAYOUT_2X1
	CP_LAYOUT_1P2HOR
	CP_LAYOUT_1P2HOR_UP
	CP_LAYOUT_1P2VER
	CP_LAYOUT_2X2
	CP_LAYOUT_1P3HOR_UP
	CP_LAYOUT_1P3VER
	CP_LAYOUT_1P4HOR_UP

Table 4-9 LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values (Continued)

Layout	Flag Value
	CP_LAYOUT_1P4HOR
	CP_LAYOUT_1P4VER
	CP_LAYOUT_1P5
	CP_LAYOUT_1P7
	CP_LAYOUT_1P8UP
	CP_LAYOUT_1P8CENT
	CP_LAYOUT_1P8HOR_UP
	CP_LAYOUT_3X3
	CP_LAYOUT_2P8
	CP_LAYOUT_1P12
	CP_LAYOUT_4X4

4 Click **OK**.
The flag is updated in the *MCMS_PARAMETERS* list.

5 Click **OK**.

For flag changes (including deletion) to take effect, reset the MCU. For more information see "*Resetting the RMX"* on page **21-69**.

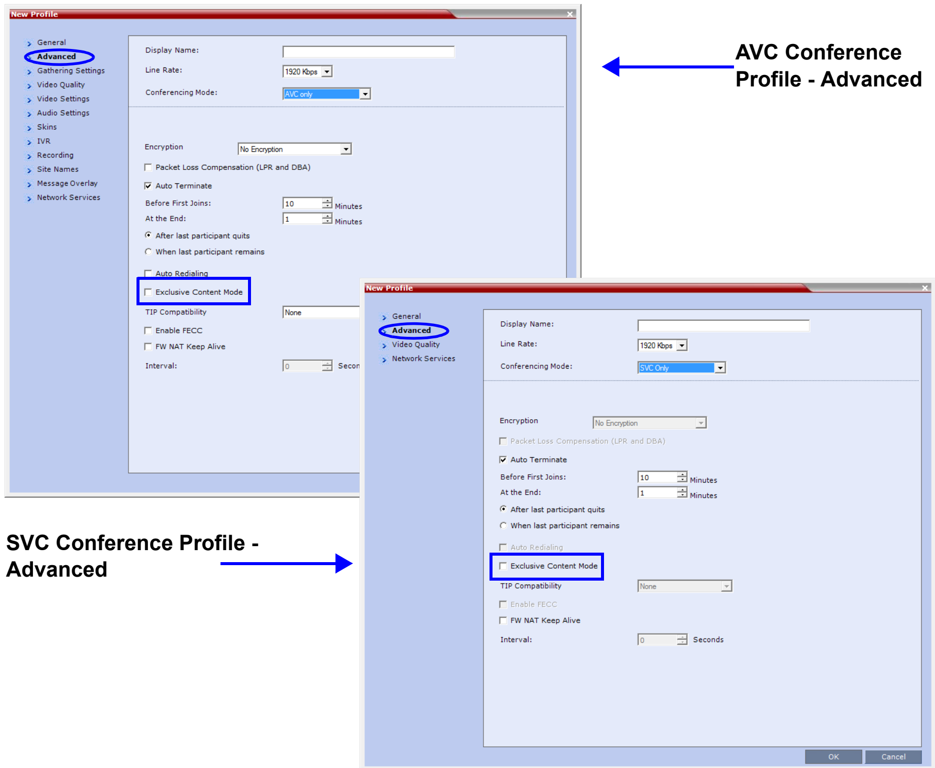
Exclusive Content Mode

Exclusive Content Mode allows you to limit *Content* broadcasting to one participant, preventing other participants from interrupting the *Content* broadcasting while it is active.

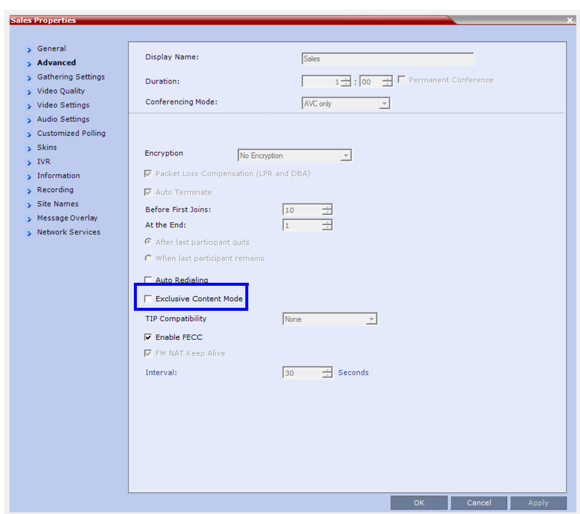
Guidelines

- *Exclusive Content Mode* is available in AVC and SVC Conferencing Modes.

- The *Exclusive Content Mode* is enabled or disabled by a check box in the in the *Advanced* tabs of the *Conference Profile*. The check box is cleared (feature is disabled) by default.



- *Exclusive Content Mode* can be enabled or disabled during an ongoing conference using the *Conference Properties - Advanced* dialog box.



- In *Exclusive Content Mode,* if the RESTRICT_CONTENT_BROADCAST _ TO_LECTURER *System Flag* is set to:
  — **NO** - the first participant to send content becomes the *Content Token* holder and has to release the *Content Token* before any other participant can acquire the token and begin transmitting *Content*.

— **YES** - only the designated *Lecturer* can be the *Content Token* holder.

- The *Exclusive Content Mode* check box replaces the EXCLUSIVE_CONTENT_ MODE *System Flag* which was used to control *Exclusive Content Mode* for the system in previous versions.
- In *Exclusive Content Mode*, if an endpoint attempts to send *Content* a few seconds after another endpoint sent *Content*, the *Content* stream it is receiving is momentarily interrupted by a slide which is displayed for a few seconds before the normal *Content* stream is resumed.

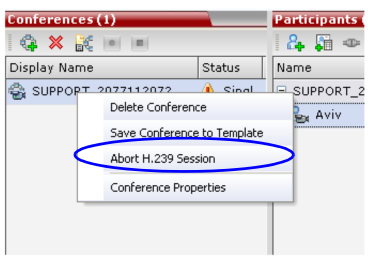
Stopping a Content Session

In some cases, when one participant ends the Content session from his/her endpoint, the Content token is not released and other participants cannot send Content.

The RMX User can withdraw the Content token from the current holder and to return it to the MCU for assignment to other endpoints.

To end the current Content session:

>> In the *Conferences* list pane, right-click the conference icon and then click **Abort H.239 Session**.



Content Broadcast Control

Content Broadcast Control prevents the accidental interruption or termination of *H.239 Content* that is being shared in a conference.

Content Broadcast Control achieves this by giving *Content Token* ownership to a specific endpoint via the *RMX Web Client*. Other endpoints are not able to send content until *Content Token* ownership has been transferred to another endpoint via the *RMX Web Client*.

Guidelines

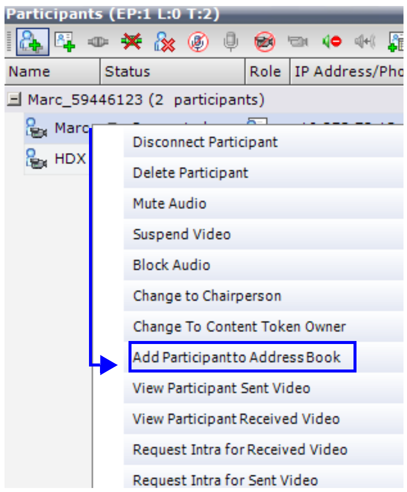
- *Content Broadcast Control* is supported in *MPM+* and *MPMx* card configuration modes.
- *Content Broadcast Control* is supported in *CP* and *Video Switching* conferences.
- *Content Broadcast Control* is supported in H.323 environments.
- Only the selected *Content Token* owner may send content and *Content Token* requests from other endpoints are rejected.
- *Content Token* ownership is valid until:
  — It is canceled by the RMX User via the *RMX Web Client.*
  — The owner releases it.
  — The endpoint of the *Content Token* owner disconnects from the conference.
- The RMX User can cancel *Content Token* ownership.

- In cascaded conferences, a participant functioning as the cascade link cannot be given token ownership.

Giving and Cancelling Token Ownership

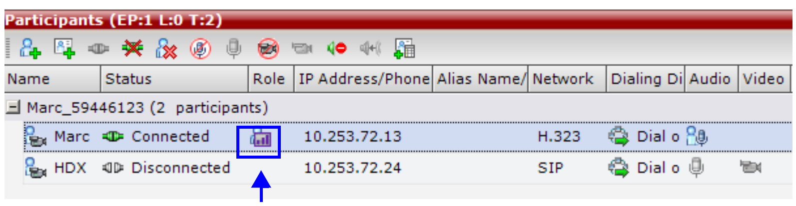
To give token ownership:

1 In the Participants list, right click the endpoint that is to receive Content Token ownership.



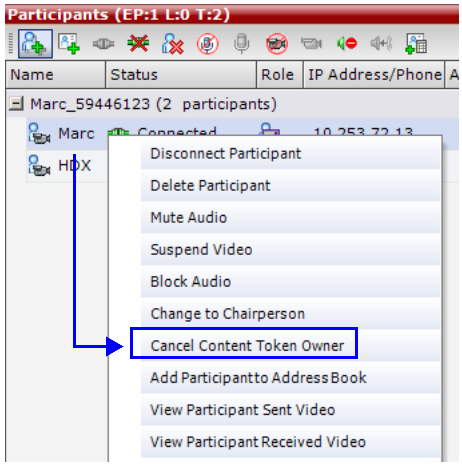
2 Select **Change To Content Token Owner** in the drop-down menu.

The endpoint receives ownership of the *Content Token* and an indication icon is displayed in the Role column of the participant's entry in the Participants list.



To cancel token ownership:

1 In the *Participants* list, right click the endpoint that currently has *Content Token* ownership.



2 Select **Cancel Content Token Owner** in the drop-down menu.
Content Token ownership is cancelled for the endpoint.

Managing Noisy Content Connections

The system can identify participants who send frequent requests to refresh their Content display usually as a result of a problematic network connection. The frequent refresh requests cause frequent refresh of the Content display and degrade the viewing quality.

When the system identifies the noisy participants, the system will automatically suspend the requests to refresh the sent Content to avoid affecting the quality of the Content viewed by other conference participants. This process is controlled by System flags.

Content Display Flags

- **MAX_INTRA_REQUESTS_PER_INTERVAL_CONTENT**
  Enter the maximum number of refresh (intra) requests for the Content channel sent by the participant's endpoint in a 10 seconds interval that will be dealt by the RMX system. When this number is exceeded, the Content sent by this participant will be identified as noisy and his/her requests to refresh the Content display will be suspended.
  Default setting: 3
- **MAX_INTRA_SUPPRESSION_DURATION_IN_SECONDS_CONTENT**
  Enter the duration in seconds to ignore the participant's requests to refresh the Content display.
  Default setting: 10
- **CONTENT_SPEAKER_INTRA_SUPPRESSION_IN_SECONDS**
  This flag controls the requests to refresh (intra) the Content sent from the RMX system to the Content sender as a result of refresh requests initiated by other conference participants.

Enter the interval in seconds between the Intra requests sent from the RMX to the endpoint sending the Content to refresh the Content display. Refresh requests that will be received from endpoints within the defined interval will be postponed to the next interval.
Default setting: 5

Forcing Other Content Capabilities

- The **H239_FORCE_CAPABILITIES** *System Flag* in *system.cfg* gives additional control over Content sharing:
  - When the flag is set to **NO (default)**, the RMX only verifies that the endpoint supports the content protocols: *H.263* or *H.264*.
  - When set to **YES**, the RMX checks frame rate, bit rate, resolution, annexes and all other parameters of the Content mode as declared by an endpoint during the capabilities negotiation phase. If the endpoint does not support the Content capabilities of the MCU, the participant will not be able to send or receive content over a dedicated content channel.

Video Preview

RMX users can preview the video sent from the participant to the conference (MCU) and the video sent from the conference to the participant. It enables the RMX users to monitor the quality of the video sent and received by the participant and identify possible quality degradation.

The video preview is displayed in a separate window independent to the *RMX Web Client*. All Web Client functionality is enabled and conference and participant monitoring as well as all other user actions can be performed while the video preview window is open and active. Live video is shown in the preview window as long as the window is open. The preview window closes automatically when the conference ends or when participant disconnects from the conference. It can also be closed manually by the RMX user.

Video Preview Guidelines

- Video preview is available in *AVC* (CP and VSW) conferences. It is not available in *SVC* Conferencing Mode.
- Video preview window size and resolution are adjusted to the resolution of the PC that displays the preview.
- Video Preview of the video sent from the conference to the participant is shown according to the line rate and video parameters of the level threshold to which the participant is connected.
- In versions up to and including Version 7.2.2, only users with Administrator authorization could request to view a video preview. In later versions, all users can view a video preview.
- Video preview is supported with MPM+ and MPMx cards.
- Only one preview window can be displayed for each *RMX Web Client* connection (workstation).

- Only one preview window can be displayed for a single conference and up to four preview windows can be displayed for each media card on different workstations (one per workstation and one per conference). For example, if the RMX contains two media cards, and there are 5 conferences running on the RMX, if five conferences are running on the same media card, only four conferences can be previewed from four different workstations. If four or less conferences are running on one media card and the remaining conferences are running on the other media card, all five conferences can be previewed.
- Live video that is shown in the preview window does not include the Content when it is sent by the participant.
- Video Preview is supported in cascaded conferences.
- If the video preview window is opened when the IVR slide is displayed to the participant, it will also be displayed in the video preview window.
- Video Preview is not supported in RMX Manager application.
- Video Preview is supported with *H.264 High Profile* in *CP conferences* only.
- Video Preview is not supported for endpoints using the *RTV* protocol.
- Video Preview is disabled in encrypted conferences.
- Video preview cannot be displayed when the participant's video is suspended.
- Participant's video preview and the CMAD window cannot be open and running simultaneously on the same PC as both require the same DirectDraw resource.

Workstation Requirements

To be able to display the video preview window, the following minimum requirements must be met:

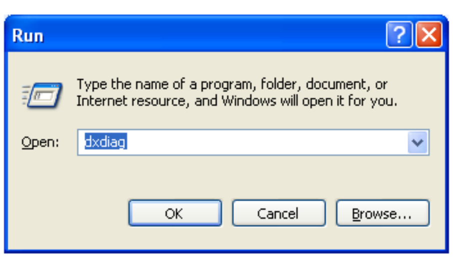
- Windows XP and later
- Internet Explorer 7
- DirectX is installed
- DirectDraw Acceleration must be enabled and no other application is using the video resource
- Hardware acceleration must be enabled

Testing your Workstation

To ensure that your workstation can display the video preview window:

1 In Windows, click **Start > Run**.
The *Run* dialog box opens.

2 In the *Open* field, type **dxdiag** and press the **Enter** key or click **OK**.

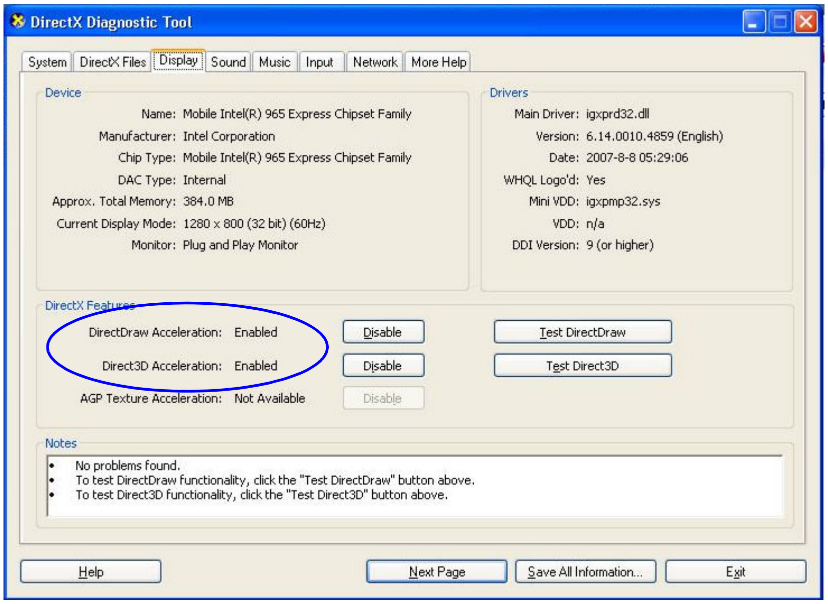


A confirmation message is displayed.

3 Click **Yes** to run the diagnostics.
The *DirectX Diagnostic Tool* dialog box opens.

4 Click the **Display** tab.

To be able to display the video preview window, the **DirectDraw Acceleration** and **Direct3D Acceleration** options must be **Enabled**.



If the video card installed in the PC does not support DirectDraw Acceleration, a black window may be viewed in the Video Preview window.

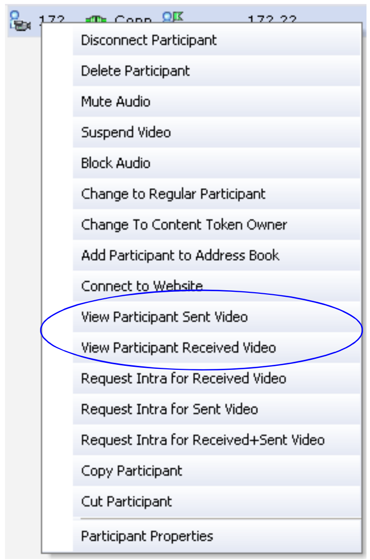
5 Click the **Exit** button.

Previewing the Participant Video

To preview the participant video:

1 List the conference participants in the *Participants* pane.

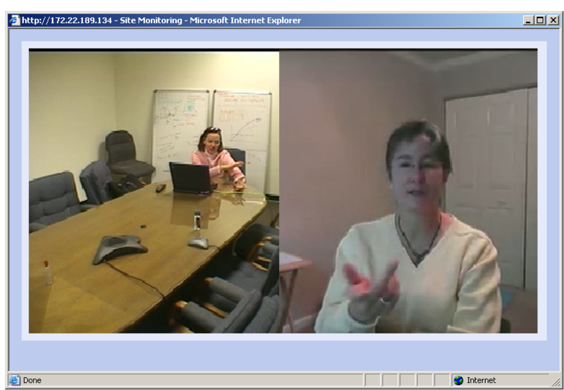
2 Right-click the participant whose video you want to preview and then click one of the following options:



— **View Participant Sent Video** - to display the video sent from the participant to the conference.

— **View Participant Received Video** - to display the video sent from the conference to the participant.

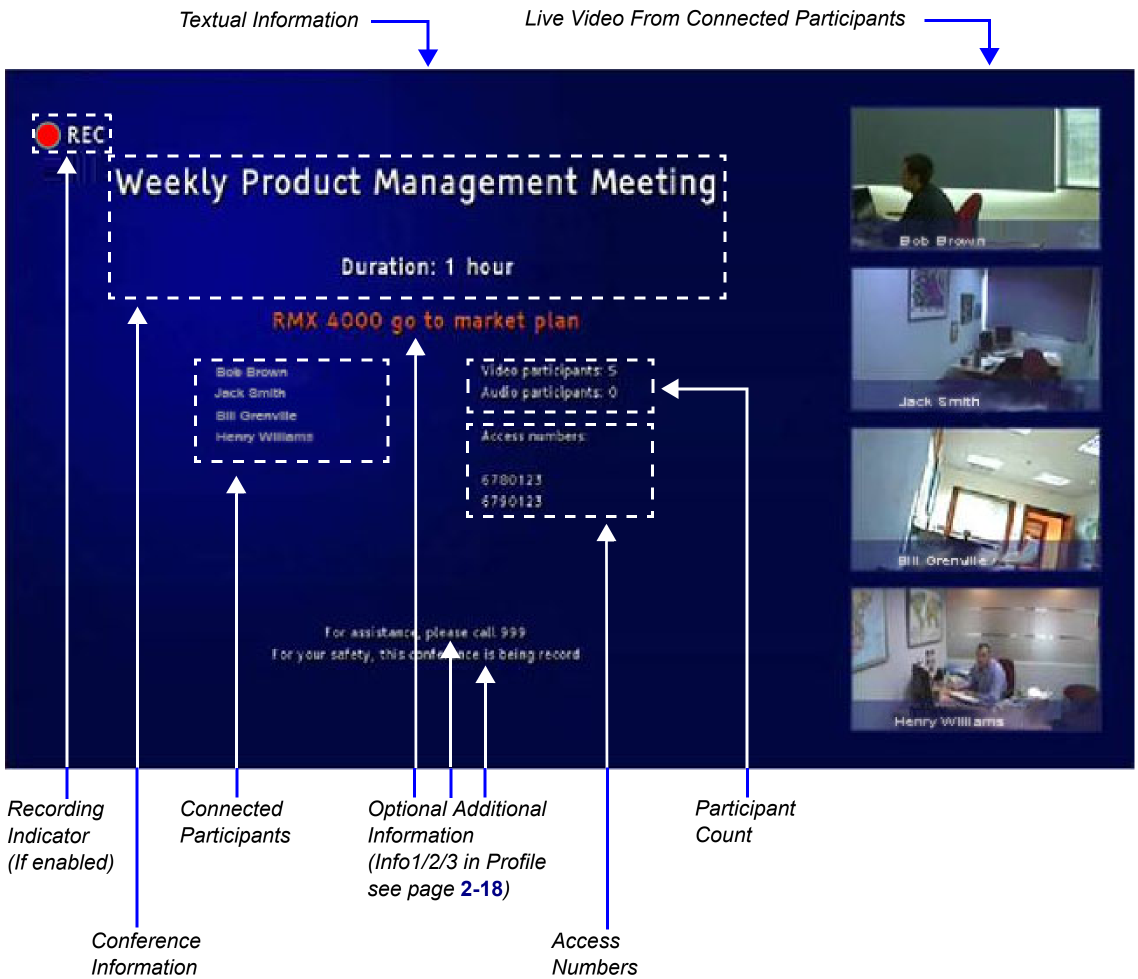
The *Video Preview* window opens.



If the video card installed in the PC does not support DirectDraw Acceleration, a black window may be viewed.

Gathering Phase

The *Gathering Phase* of an AVC (CP only) conference is the time period during which participants are connecting to a conference. During the *Gathering Phase*, a mix of live video from connected endpoints is combined with both static and variable textual information about the conference into a slide which is displayed on all connected endpoints.

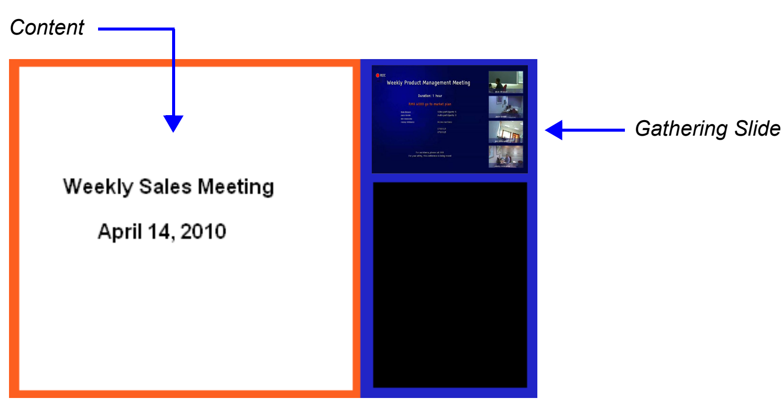


During the *Gathering Phase*, the audio of all participants can be heard, and the video of active speakers is displayed in the video windows as they begin talking.

All connected participants are kept informed about the current conference status including names of connected participants, participant count, participant type (video/audio) etc.

Gathering Phase Guidelines

- *Gathering Phase* is only available in AVC only (CP only) conferences. It is not supported in *Video Switching* conferences and *SVC Only* conferences.
- The *Gathering Phase* slide can be displayed at any time during the conference by entering the *Show Participants DTMF* code, ***88**.
  Note: When the display of the Gathering Phase slide is removed, the message overlay text is also removed.
- The names of the first eight participants to connect are displayed. If eight or more participants connect, the 8th row displays "**...**".
- **Static text** in the *Gathering Phase* slide such as the field headings: *Organizer, Duration, Video/Audio Participants, Access Number, IP* are always displayed in the language as configured in the *Polycom Virtual Meeting Rooms Add-in for Microsoft Outlook*.The following languages are supported:
  — English
  — French
  — German
  — International Spanish
  — Korean
  — Japanese
  — Simplified Chinese
- **Dynamic text** in the *Gathering Phase* slide such as the meeting name, participants' names, access numbers and the additional information entered in the *Info1/2/3* fields of the *Gathering Settings* tab of the conference *Profile* are displayed in the language of the meeting invitation.
- The language of a *Gathering Phase* slide of a conference configured to include a *Gathering Phase* that is not launched by the *Polycom Conferencing Add-in for Microsoft Outlook* is configured by the administrator. Using the *RMX Web Client,* the administrator selects the language for the *Gathering Phase slide.* The language selected can be different to that of the *RMX Web Client* used by the administrator to perform the configuration.
- *Content* can be sent during the *Gathering Phase.* The content is displayed in the large video window of the participant's layout while the *Gathering* slide is displayed in a smaller video window in the layout.



Gathering Phase Duration

The duration of the *Gathering Phase* can be customized by the administrator so that it is long enough to be viewed by most connected participants yet short enough so as not to over extend into the scheduled conferencing time.

The *Gathering Phase* duration is configured for the RMX, by the following *System Flags* in *system.cfg* using the *Setup >System Configuration* menu:

- **CONF_GATHERING_DURATION_SECONDS**

  Range: 0 - 3600 seconds

  Default: 180 seconds

  The *Gathering Phase* duration of the conference is measured from the scheduled start time of the conference.

  Example: If the value of the flag is set to **180**, the *Gathering* slide is displayed for three minutes to all participants starting at the conference *Start Time*, and ending three minutes after the conference *Start Time*.

  For participants who connect before *Start Time*, the *Gathering* slide is displayed from the time of connection until the end of the *Gathering* duration period.

- **PARTY_GATHERING_DURATION_SECONDS**

  Range: 0 - 3600 seconds

  Default: 15 seconds

  The value of this flag determines the duration of the display of the *Gathering* slide for participants that connect to the conference after the conference *Start Time*.

  Participants connecting to the conference very close to of the end of the *Gathering Phase* (when there are fewer seconds left to the end of the *Gathering Phase* than specified by the value of the flag) have the *Gathering* slide displayed for the time specified by the value of the flag.

  Example: If the value of the flag is set to **15**, the *Gathering Phase* slide is displayed to the participant for 15 seconds.

Enabling the Gathering Phase Display

The *Gathering Phase* is enabled for per conference in the *Conference Profile*. The profile also includes the dial-in numbers and the optional additional information to display on the slide.

Conferences that are configured to include a *Gathering Phase* that are not launched by the *Polycom Conferencing Add-in for Microsoft Outlook* need the following information to be entered via the *New Profile* or *Profile Properties – Gathering Settings* dialog box:

- *Display Name* (Optional, the *Meeting Name* is used if left blank.)
- *Displayed Language*
- *Access Number 1 / 2* (Optional.)
- Additional Information (Optional free text)
  - — *Info 1*
  - — *Info 2*
  - — *Info 3*

Conferences launched by the *Polycom Conferencing Add-in for Microsoft Outlook* receive this information from the meeting invitation.

For more information see "*Defining New Profiles*" on page **2-18**.

Auto Scan and Customized Polling in Video Layout

Auto Scan enables a user to define a single cell in the conference layout to cycle the display of participants that are not in the conference layout.

Customized Polling allows the cyclic display to be set to a predefined order for a predefined time period. The cyclic display only occurs when the number of participants is larger than the number of cells in the layout.

Guidelines

- *Auto Scan* and *Customized Polling* are supported in AVC - CP conferences only.
- Participants that are in the conference layout will not appear in the *Auto Scan* enabled cell.
- If *Customized Polling* is not used to define the order of the *Auto Scan* it will proceed according to order in which the participants connected to the conference.
- If the user changes the conference layout, the *Auto Scan* settings are not exported to the new layout. If the user changes the conference layout back to the layout in which *Auto Scan* was enabled, *Auto Scan* with the previous settings will be resumed.

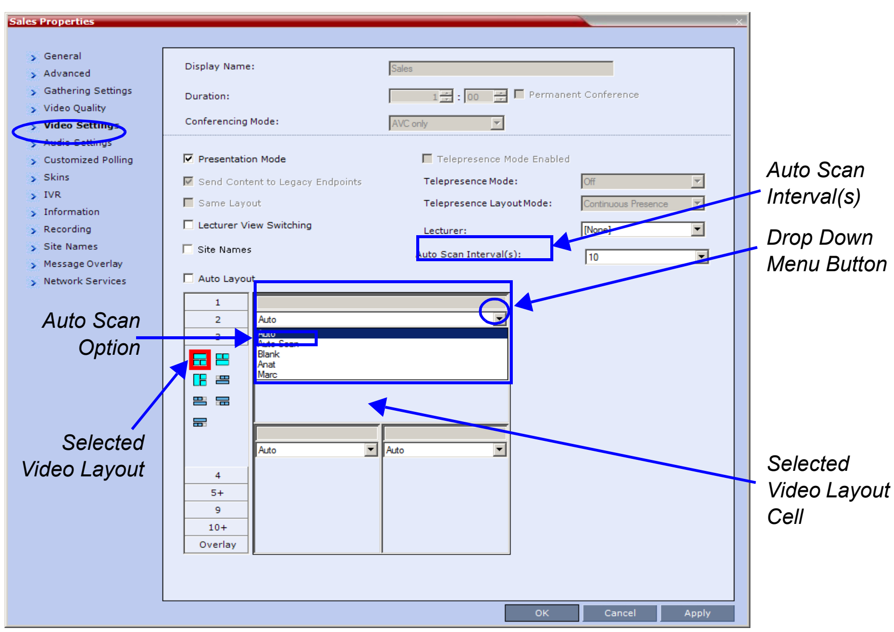
Enabling Auto Scan and Customized Polling

Auto Scan

To enable Auto Scan:

1 In the *RMX Web Client Main Screen - Conference* list pane, double-click the conference or right-click the conference and then click **Conference Properties**.

2 In the *Conference Properties - General* dialog box, click **Video Settings**.
The *Video Settings* tab is displayed.



3 In the video layout cell to be designated for *Auto Scan*, click the drop-down menu button and select **Auto Scan**.

4 Select from the *Auto Scan Interval(s)* drop-down list the scanning interval in seconds.

5 Click the **Apply** button to confirm and keep the *Conference Properties* dialog box open.

-or-

Click **OK** to confirm and close the *Conference Properties* dialog box.

Customized Polling

The order in which the Auto Scanned participants are displayed in the *Auto Scan* enabled cell of the video layout can be customized.

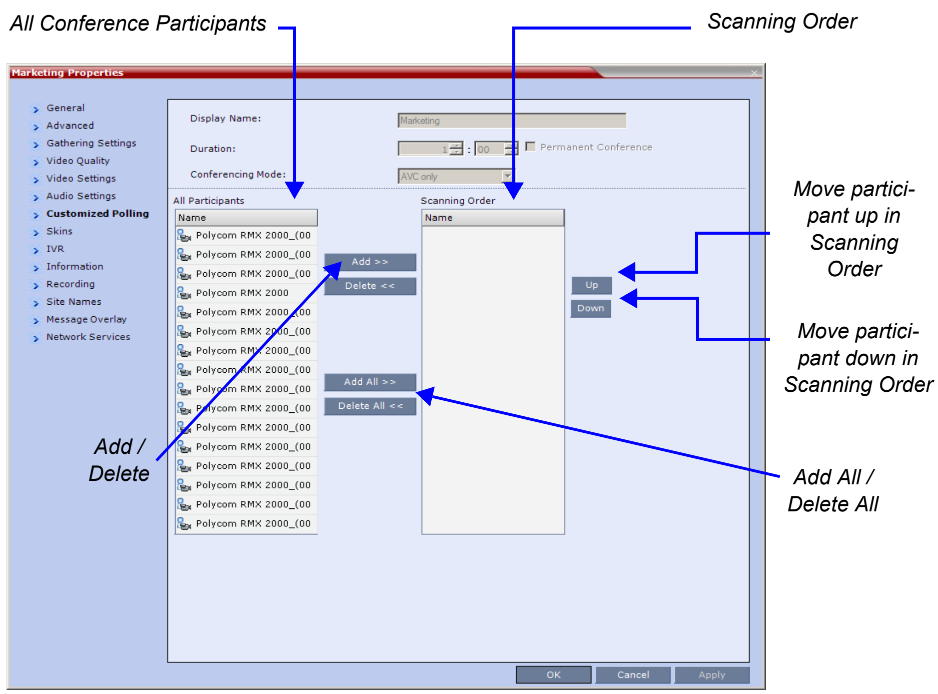
1 Open the *Customized Polling* tab:

a If the *Video Settings* tab is open click the **Customized Polling** tab.

or

b In the *Conference* list pane, double-click the conference or right-click the conference and then click **Conference Properties**.

c In the *Conference Properties - General* dialog box, click **Customized Polling**. The *Customized Polling* tab is displayed.



All conference participants are listed in the left pane (*All Participants*) while the participants that are to be displayed in the Auto Scan enabled cell of the video layout are listed in the right pane (*Scanning Order*).

The dialog box buttons are summarized in Table 4-10.

***Table 4-10** Customized Polling - Buttons*

Button	Description
Add	Select a participant and click this button to *Add* a the participant to the list of participants to be Auto Scanned. The participants name is removed from the *All Participants* pane.
Delete	Select a participant and click this button to *Delete* the participant from the list of participants to be *Auto Scanned*. The participants name is moved back to the *All Participants* pane.
Add All	Add all participants to the list of participants to be *Auto Scanned*. All participants' names are removed from the *All Participants* pane.
Delete All	Delete all participant from the list of participants to be *Auto Scanned*. All participants' names are moved back to the *All Participants* pane.
Up	Select a participant and click this button to move the participant *Up* in the *Scanning Order*.
Down	Select a participant and click this button to move the participant *Down* in the *Scanning Order*.

2 **Optional.** Add a participant to the list of participants to be *Auto Scanned*:
   — Click on the participant's name in the *All Participants* list and then click the **Add** button to move the participant to the *Scanning Order* pane.

3 **Optional.** Delete a participant from the list of participants to be *Auto Scanned*:
   — Click on a participant's name in the *Scanning Order* list and then click the **Delete** button to move the participant back to the *All Participants* pane.

4 **Optional.** Add all participants to the list of participants to be *Auto Scanned* by clicking the **Add All** button.

5 **Optional.** Delete all participant from the list of participants to be *Auto Scanned* by clicking the **Delete All** button.

6 **Optional.** Move the participant up in the *Scanning Order* by clicking the **Up** button.

7 **Optional.** Move the participant down in the *Scanning Order* by clicking the **Down** button.

8 Click the **Apply** button to confirm and keep the *Conference Properties* dialog box open, or click the **OK** the button to confirm and return to the *RMX Web Client Main Screen*.

Audio Algorithm Support

The RMX supports the following audio algorithms in **AVC conferences:** G.711, G. 719, G.722, G.722.1, G.722.1C, G. 728, G.729A, G.723.1, Siren14, Siren 22 and SirenLPR.

Polycom's proprietary *Siren 22* and industry standard *G.719* audio algorithms are supported for participants connecting with *Polycom* endpoints.

The *Siren 22* audio algorithm provides CD-quality audio for better clarity and less listener fatigue with audio and visual communication applications. *Siren 22* requires less computing power and has much lower latency than alternative wideband audio technologies.

The SirenLPR audio algorithm provides CD-quality audio for better clarity and less listener fatigue with audio and visual communication applications.

In **SVC conferences**, the system supports SAC (Scalable Audio Coding) audio algorithm.

Guidelines

- *Siren 22, G.719* and *Siren 22Stereo* are supported with *MPM+* and *MPMx* cards.
- *Siren 22* and *G.719* are supported in both mono and stereo.
- Stereo is supported in *H.323* calls only.
- *Siren 22* is supported by Polycom HDX endpoints, version 2.0 and later.
- *G.728* is supported with both *MPM+* and *MPMx* cards and in *H.323*, *SIP* and *ISDN* environments.
- *SirenLPR* is enabled by default and can be disabled by setting the system flag, **ENABLE_SIRENLPR**, to **NO**.
- *SirenLPR* is supported:
  — With *MPMx Cards* only.
  — In IP (H.323, SIP) calls only.
  — In CP and VSW conferences.
  — With *Polycom CMAD* and *HDX* "*Canyon 3.0.1*" endpoints.
  — For mono audio at audio line rates of 32Kbps, 48Kbps and 64Kbps.
  — For stereo audio at audio line rates of 64Kbps, 96Kbps and 128Kbps.

SIP Encryption

The **ENABLE_SIRENLPR_SIP_ENCRYPTION** *System Flag* enables the *SirenLPR* audio algorithm when using encryption with the *SIP* protocol.

The default value of this flag is **NO** meaning *SirenLPR* is disabled by default for *SIP* participants in an encrypted conference. To enable *SirenLPR* the *System Flag* must be added to *system.cfg* and its value set to **YES**.

Mono

The *Siren 22*, *G.719* and *SirenLPR* mono audio algorithms are supported at the following bit rates:

Table 4-11 *Siren22, G.719 and SirenLPR Mono vs Bitrate*

Audio Algorithm	Minimum Bitrate (kbps)
Siren22 64k	384
Siren22 48K	
Siren22_32k	
G.719_64k	
G.719_48k	
G.719_32k	
G.728 16K	

Table 4-11 *Siren22, G.719 and SirenLPR Mono vs Bitrate (Continued)*

Audio Algorithm	Minimum Bitrate (kbps)
Siren22_48K	256
Siren22_32k	
G.719_48k	
G.719_32k	
G.728 16	
Siren22_32k	128
G.719_32k	
G.728 16K	
SirenLPR	64
SirenLPR	48
SirenLPR	32

Stereo

The *Siren 22Stereo, G.719Stereo* and *SirenLPR* audio algorithms are supported at the following bit rates.

Table 4-12 *Siren22Stereo, G.719Stereo and SirenLPR vs Bitrate*

Audio Algorithm	Minimum Bitrate (kbps)
Siren22Stereo_128k	1024
Siren22Stereo_96k	
Siren22Stereo_64k	
G.719Stereo_128k	
G.719Stereo_96k	
G.719Stereo_64k	
Siren22Stereo_96k	512
Siren22Stereo_64k	
G.719Stereo_96k	
G.719Stereo_64k	
Siren22Stereo_64k	384
G.719Stereo_64k	
SirenLPR	128
SirenLPR	96
SirenLPR	64

Audio algorithms supported for ISDN

***Table 4-13** Supported Audio Algorithm vs Bitrate*

Audio Algorithm	Minimum Bitrate (kbps)
G.722.1C 48K	256
G.722.1C 32K	
G.722.1C 24K	
Siren14 48K	
Siren14 32K	
Siren14 24K	
G.722.1 32K	
G.722.1 24K	
G.722.1 16K	256
G.722 48K	
G.722 56K	
G.722 64K	
G.711 56K	
G.711 64K	
G.728 16K	
G.722.1C 32K	128
G.722.1C 24K	
Siren14 32K	
Siren14 24K	
G.722.1 32K	
G.722.1 24K	
G.722 48K	
G.722 56K	
G.722 64K	
G.711 56K	
G.711 64K	
G.728 16K	

Table 4-13 Supported Audio Algorithm vs Bitrate (Continued)

Audio Algorithm	Minimum Bitrate (kbps)
G.722.1 16K	96
G.722.1C 24K	
Siren14 24K	
G.722 48K	
G.722 56K	
G.722 64K	
G.711 56K	
G.711 64K	
G.728 16K	
G.728 16K	64

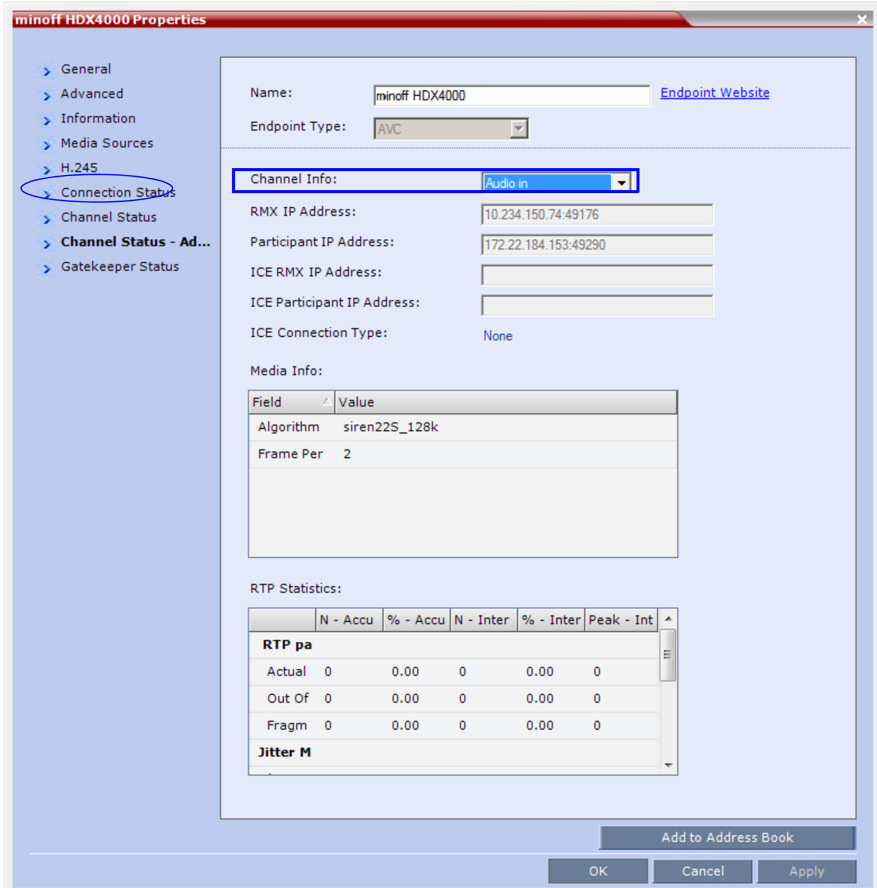
Monitoring Participant Audio Properties

The audio algorithm used by the participant's endpoint can be verified in the Participant Properties - Channel Status dialog box.

To view the participant's properties during a conference:

1. In the *Participants* list, right click the desired participant and select **Participant Properties**.
2. Click the **Channel Status - Advanced** tab.
   The *Participant Properties - Channel Status - Advanced* dialog box is displayed.

3 In the *Channel Info* field, select **Audio In** or **Audio Out** to display the audio parameters.



4 Click the **OK** button.

Media Encryption (AVC Only)

Encryption is available at the conference and participant levels, based on AES 128 (Advanced Encryption Standard) and is fully H.233/H.234 compliant and the Encryption Key exchange DH 1024-bit (Diffie-Hellman) standards.

Media Encryption Guidelines

- Encryption is not available in all countries and it is enabled in the MCU license. Contact Polycom Support to enable it.
- Media encryption is not supported in SVC Conferencing Mode.
- Endpoints must support both AES 128 encryption and DH 1024 key exchange standards which are compliant with H.235 (H.323) to encrypt and to join an encrypted conference.
- The encryption mode of the endpoints is not automatically recognized, therefore the encryption mode must be set for the conference or the participants (when defined).

- *Media Encryption* for *ISDN/PSTN* participants is implemented in RMX systems with MPM+ and MPMx cards.
- Conference level encryption must be set in the Profile, and cannot be changed once the conference is running.
- If an endpoint connected to an encrypted conference stops encrypting its media, it is disconnected from the conference.
- In Cascaded conferences, the link between the cascaded conferences must be encrypted in order to encrypt the conferences.
- *Media Encryption* for *ISDN/PSTN (H.320)* participants is not supported in cascaded conferences.
- The recording link can be encrypted when recording from an encrypted conference to the RSS that is set to encryption. For more information, see "*Recording Link Encryption"* on page **14-7**.
- Encryption of SIP Media is supported using *SRTP* (*Secured Real-time Transport Protocol*) and the *AES* key exchange method.
- Encryption of SIP Media requires the encryption of SIP signaling - TLS Transport Layer must be used.
- Encryption of SIP Media is supported in CP and VSW conferences.
  - All media channels are encrypted: video, audio and FECC.
  - Encryption of SIP Media is available only in MPM+ and MPMx Card Configuration Modes.
  - RMX SRTP implementation complies with Microsoft SRTP implementation.
  - LPR is not supported with SRTP.
  - The **ENABLE_SIRENLPR_SIP_ENCRYPTION** *System Flag* enables the *SirenLPR* audio algorithm when using encryption with the *SIP* protocol. The default value of this flag is **NO** meaning *SirenLPR* is disabled by default for *SIP* participants in an encrypted conference. To enable *SirenLPR* the *System Flag* must be added to *system.cfg* and its value set to **YES**.
  - The **SEND_SRTP_MKI** *System Flag* enables or disables the inclusion of the *MKI* field in *SRTP* packets sent by the RMX. The default value of the flag is **YES**. Add the flag to *system.cfg* and set its value set to **NO** to disable the inclusion of the *MKI* field in *SRTP* packets sent by the RMX when using endpoints that cannot decrypt *SRTP*-based audio and video streams if the *MKI* (*Master Key Identifier*) field is included in *SRTP* packets sent by the RMX. This *System Flag* should not be set to **NO** when *HDX* endpoints, *Microsoft Office Communicator* and *Lync Clients.* For more information, see "*Modifying System Flags"* on page **22-1**.

Mixing Encrypted and Non-encrypted Endpoints in one Conference

Mixing encrypted and non-encrypted endpoints in one conference is possible, based on the Encryption option “Encrypt When Possible” in the Conference Profile - Advance dialog box. The behavior is different for H.323/SIP and ISDN participants.

In versions prior to version 7.6.1, this behavior is based on the setting of the system flag ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF.

The option *"Encrypt When Possible"* enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. Defined participants that cannot connect encrypted are connected non-encrypted, with the exception of dial-out SIP participants.

- When the conference encryption is set to "*Encrypt when possible*", dial out SIP participants whose encryption is set to AUTO can only connect with encryption, otherwise they are disconnected from the conference.
- In CISCO SIP environments, dial in endpoints that are registered to CUCM can only connect as non-encrypted when the conference encryption is set to "*Encrypt when possible*" as the CUCM server sends the Invite command without SDP.

The same system behavior can be applied to undefined participants, depending on the setting of the System Flag FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE:

- When set to **NO** and the conference encryption in the Profile is set to *"Encrypt When Possible"*, both *Encrypted* and *Non-encrypted undefined participants* can connect to the same conferences, where encryption is the preferred setting.
- When set to **YES** (default), *Undefined participants* must connect encrypted, otherwise they are disconnected.

For *defined participants*, connection to the conference is decided according to the encryption settings in the conference *Profile,* the *Defined Participant's* encryption settings.

For *undefined participants*, connection to the conference is decided according to the encryption settings in the conference *Profile,* the System Flag setting and the connecting endpoint's *Media Encryption* capabilities.

Direct Connection to the Conference

Table 4-14, summarizes the connection status of participants, based on the encryption settings in the conference *Profile,* the *Defined Participant's* encryption settings or the System Flag setting for undefined participants and the connecting endpoint's *Media Encryption* capabilities.

Table 4-14 *Connection of Defined and Undefined H.323, SIP and ISDN Participants to the Conference Based on the Encryption Settings*

Conference Encryption Setting	Defined Participant		Undefined Participant	
	Encryption Setting	Connection status	Connection Status *Flag = No	Connection Status *Flag = YES
No Encryption	**Auto**	Connected, non-encrypted	Connected non-encrypted (Encryption is not declared by the RMX, therefore the endpoint does not use encryption)	Connected non-encrypted (Encryption is not declared by the RMX, therefore the endpoint does not use encryption)
	No	Connected, non-encrypted		
	Yes	Connected only if encrypted. Non-encrypted endpoints are disconnected as encryption is forced for the participant.		

Table 4-14 Connection of Defined and Undefined H.323, SIP and ISDN Participants to the Conference Based on the Encryption Settings (Continued)

Conference Encryption Setting	Defined Participant		Undefined Participant	
	Encryption Setting	**Connection status**	**Connection Status *Flag = No**	**Connection Status *Flag = YES**
Encrypt All	**Auto**	Connected, encrypted. Non-encrypted endpoints are disconnected	Connect only if encrypted. Non-encrypted endpoints are disconnected	Connect only if encrypted. Non-encrypted endpoints are disconnected
	No	Disconnected (cannot be added to the conference)		
	Yes	Connected, encrypted		
Encrypt When Possible	**Auto**	*All defined participants **except** dial-out SIP participants:* Connect encrypted - Endpoints with encryption capabilities. Connect non-encrypted - endpoints without encryption capabilities. *Defined dial-out SIP participant:* Connect only if encrypted. Non-encrypted endpoints are disconnected.	Connect encrypted - Endpoints with encryption capabilities. Connect non-encrypted - endpoints without encryption capabilities	Connect only if encrypted. Non-encrypted endpoints are disconnected.
	No	Connected, non-encrypted		
	Yes	Connected, encrypted		

* System Flag = FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE

Connection to the Entry Queue

An undefined participant connecting to an *Entry Queue* inherits the encryption characteristics of the *Entry Queue* as defined in the *Entry Queue's* profile.

Table 4-15 summarizes the connection possibilities for a participant that is to be moved from an *Entry Queue* to a destination conference for each of the conference *Profile* and Entry Queue encryption options.

Table 4-15 Connection of Undefined Participants to the Entry Queue Based on the Encryption Settings

Entry Queue Encryption Setting	Undefined Participant Connection to the Entry Queue	
	***Flag = No**	***Flag = YES**
No Encryption	Connected, non-encrypted (Encryption is not declared by the RMX, therefore endpoint does not use encryption)	Connected, non-encrypted (Encryption is not declared by the RMX, therefore endpoint does not use encryption)

Table 4-15 Connection of Undefined Participants to the Entry Queue Based on the Encryption Settings (Continued)

Entry Queue Encryption Setting	Undefined Participant Connection to the Entry Queue	
	*Flag = No	*Flag = YES
Encrypt All	Connected only if encrypted. Non-encrypted endpoints are disconnected	Connected only if encrypted. Non-encrypted endpoints are disconnected
Encrypt When Possible	Connected encrypted - Endpoints with encryption capabilities. Connected non-encrypted - endpoints without encryption capabilities	Connected only if encrypted. Non-encrypted endpoints are disconnected.

* System Flag = FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE

Moving from the Entry Queue to Conferences or Between Conferences

When moving from the Entry Queue to the destination conference, or when the RMX user moves participants from one conference to another, the connection rules are similar and they are summarized in Table 4-16:

Table 4-16 Moving Participants from the Entry Queue to the Destination conference or between conferences Based on the Encryption Settings

Destination Conference Encryption Setting	Current Participant Encryption Status			
	Encrypted		Non-Encrypted	
	*Flag = NO	*Flag = YES	*Flag = NO	*Flag = YES
No Encryption	Move succeeds, connected encrypted		Move succeeds, connected non-encrypted	
Encrypt All	Move succeeds, connected encrypted.		Move fails, disconnected.	
Encrypt When Possible	Move succeeds, connected encrypted	Move succeeds, connected encrypted	Move succeeds, connected non-encrypted	Connected only if endpoint was a defined participant in the source conference. Otherwise, move fails.

* System Flag = FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE

Recording Link Encryption

Recording Links are treated as regular participants, however the ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF *System Flag* must be set to YES if a non-encrypted *Recording Link* is to be allowed to connect to an encrypted conference.

Table 4-17 summarizes the connection possibilities for a *Recording Link* that is to be connected to a conference for each of the conference *profile* and *Entry Queue* encryption options.

Table 4-17 *Connections by Recording Link and Conference Encryption Settings*

Conference Profile Setting	Recording Link Connection Status according to flag: ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF	
	YES	**NO**
Encrypt All	Connected encrypted if possible, otherwise connected non-encrypted.	Connected only if encrypted, otherwise disconnected
No Encryption	Connected non-encrypted	Connected non-encrypted
Encrypt when possible	Connected encrypted if possible, otherwise connected non-encrypted.	Connected encrypted if possible, otherwise connected non-encrypted.

Encryption Flag Settings

To modify the Encryption flags:

1 Click **Setup>System Configuration**.
The *System Flags* dialog box opens.

2 In *Version 7.6.1* and later:
Set the **FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE** flag to **YES** or **NO**.

In *Version 7.6* and earlier:
Set the **ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF** flag to **YES** or **NO**.

3 If recording will be used in encrypted conferences, set the **ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF** flag to **YES** or **NO**.

4 Click **OK**.

For more information, see "*Modifying System Flags*" on page **22-1**.

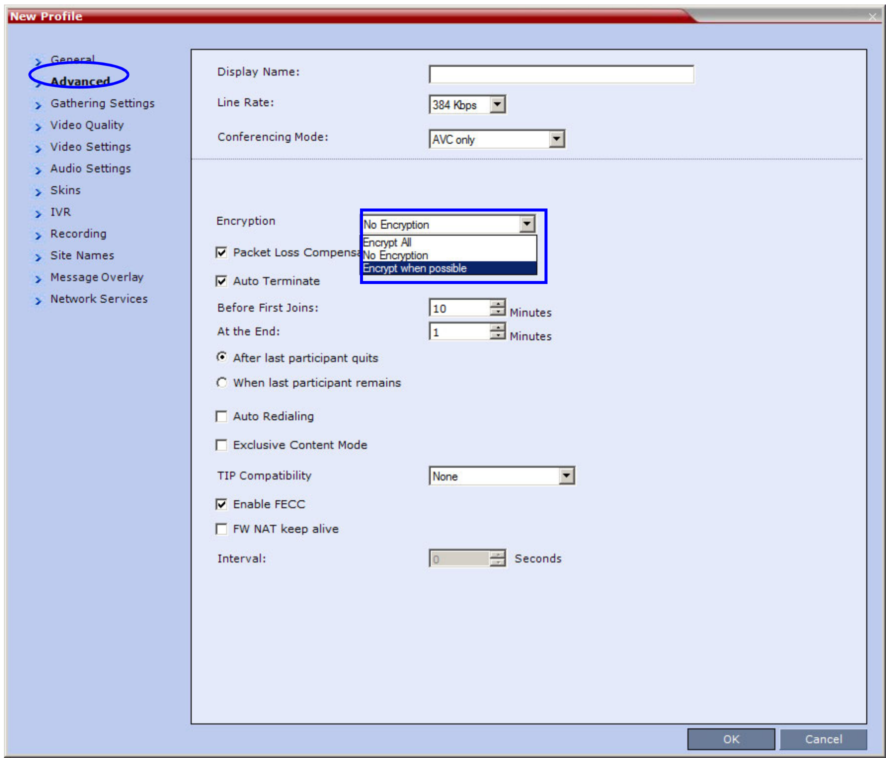
>> Reset the MCU for flag changes to take effect.

Enabling Encryption in the Profile

Encryption for the conference is in the Profile and cannot be changed once the conference is running.

To enable encryption at the conference level:

\>> In the *Conference Profile Properties – Advanced* dialog box, select one of the following Encryption options:



— **Encrypt All** - Encryption is enabled for the conference and all conference participants must be encrypted.

— **No Encryption** - Encryption is disabled for the conference.

— **Encrypt when possible** - enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. For connection guidelines see "*Mixing Encrypted and Non-encrypted Endpoints in one Conference"* on page **4-41**.

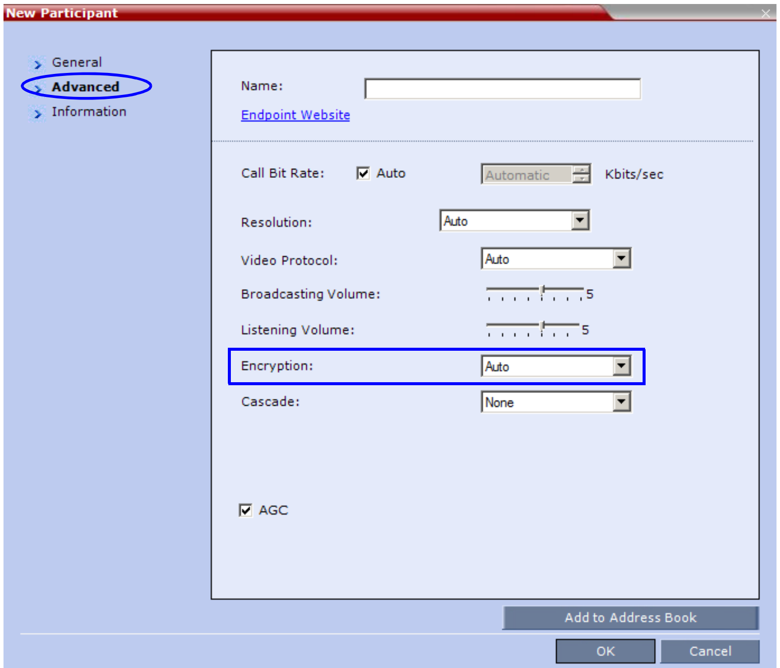
For more information about recording encrypted conferences, see "*Recording Link Encryption"* on page **14-7**.

Enabling Encryption at the Participant Level

You can select the encryption mode for each of the defined participants. Encryption options are affected by the settings of the flag in the system configuration. Undefined participants are connected with the Participant *Encryption* option set to **Auto**, inheriting the conference/ Entry Queue encryption setting.

To enable encryption at the participant level:

>> In the *Participant Properties – Advanced* dialog box, in the *Encryption* list, select one of the following options: **Auto**, **On**, or **Off**.



— **Auto** - The participant inherits the conference/Entry Queue encryption setting. The participant connects as encrypted only if the conference is defined as encrypted.

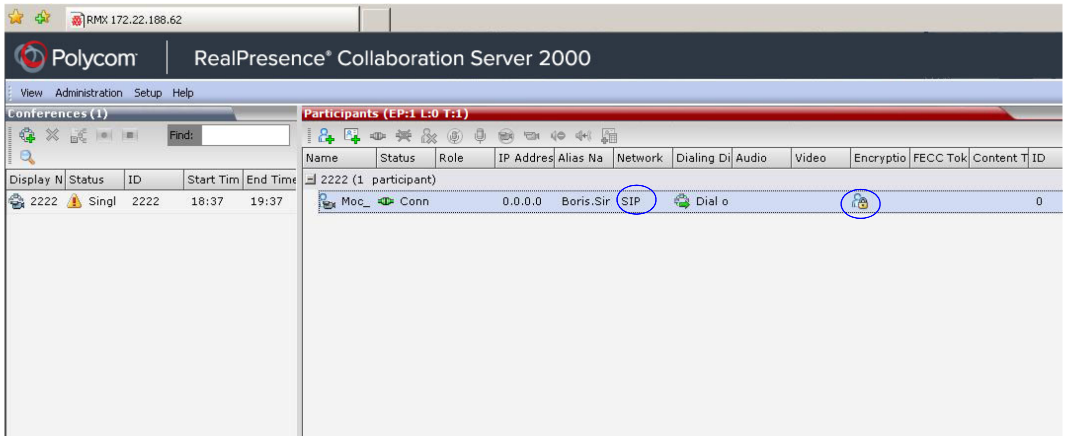
— **Yes** - The participant joins the conference/Entry Queue as *encrypted.*

— **No** - The participant joins the conference/Entry Queue as *non-encrypted*.

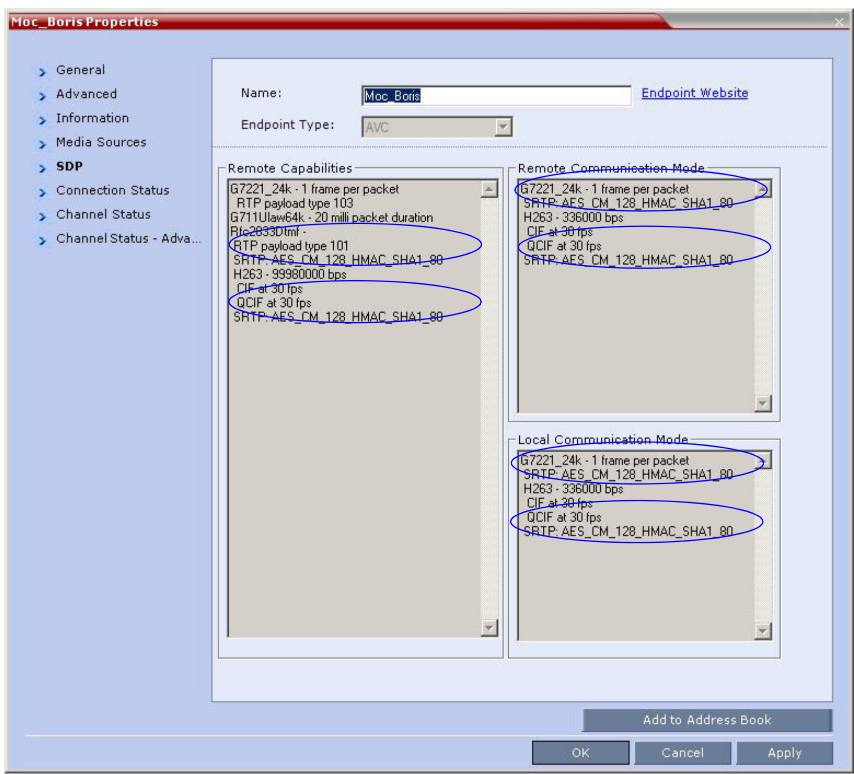
Monitoring the Encryption Status

The conference encryption status is indicated in the *Conference Properties - General* dialog box.

The participant encryption status is indicated by a check mark in the *Encryption* column in the *Participants* list pane.



The participant encryption status is also indicated in the *Participant Properties – SDP* tab, where SRTP indication is listed for each encrypted channel (for example, audio and video).



An encrypted participant who is unable to join a conference is disconnected from the conference. The disconnection cause is displayed in the *Participant Properties – Connection Status* tab, *Security Failure* indication, and the *Cause* box identifies the encryption related situation.

For more information about monitoring, see "*Conference and Participant Monitoring*" on page **13-1**.

Packet Loss Compensation (LPR and DBA)

Lost Packet Recovery (*LPR*) and *Dynamic Bandwidth Allocation* (*DBA*) help minimize media quality degradation that can result from packet loss in the network. *Packet loss Compensation* is available in *AVC Conferencing Mode* only and is not supported in *SVC Conferencing Mode*.

Packet Loss

Packet Loss refers to the failure of data packets, transmitted over an IP network, to arrive at their destination. *Packet Loss* is described as a percentage of the total packets transmitted.

Causes of Packet Loss

Network congestion within a LAN or WAN, faulty or incorrectly configured network equipment or faulty cabling are among the many causes of Packet Loss.

Effects of Packet Loss on Conferences

Packet Loss affects the quality of:

- **Video –** frozen images, decreased frame rate, flickering, tiling, distortion, smearing, loss of lip sync
- **Audio –** drop-outs, chirping, audio distortion
- **Content –** frozen images, blurring, distortion, slow screen refresh rate

Lost Packet Recovery

The *Lost Packet Recovery* (*LPR*) algorithm uses *Forward Error Correction* (*FEC*) to create additional packets that contain recovery information. These additional packets are used to reconstruct packets that are lost, for whatever reason, during transmission. *Dynamic Bandwidth Allocation* (*DBA*) is used to allocate the bandwidth needed to transmit the additional packets.

Lost Packet Recovery Guidelines

- If packet loss is detected in the packet transmissions of either the video or Content streams:
  — *LPR* is applied to both the video and Content streams.
  — *DBA* allocates bandwidth from the video stream for the insertion of additional packets containing recovery information.
- *LPR* is supported in H.323 and *SIP* networking environments only.
- In *LPR*-enabled *Continuous Presence* conferences:
  — Both *LPR*-enabled and non-*LPR*-enabled endpoints are supported.
  — The *LPR* process is not applied to packet transmissions from non-*LPR*-enabled H.323, SIP and H.320 endpoints.
  — Non-*LPR*-enabled endpoints can be moved to *LPR*-enabled conferences and *LPR*-enabled participants can be moved to conferences without *LPR*-enabled (where they remain LPR-enabled).

- In *LPR*-enabled *Video Switched* conferences:
  - — H.323 and SIP endpoints are supported.
  - — When cascading between conferences running on RMX and *MGC* (*Polycom* legacy *MCU*), *LPR* is not supported over the link between the two conferences.
  - — Non-H.323 participants cannot be created, added or moved to *LPR*-enabled *Video Switched* conferences.
- When connecting via an *Entry Queue:*
  - — A participant using an *LPR*-enabled endpoint can be moved to a non-*LPR*-enabled conference. The participant is connected with LPR enabled.
  - — SIP and H.320 participants cannot be moved to *LPR*-enabled *Video Switched* conferences.

Enabling Lost Packet Recovery

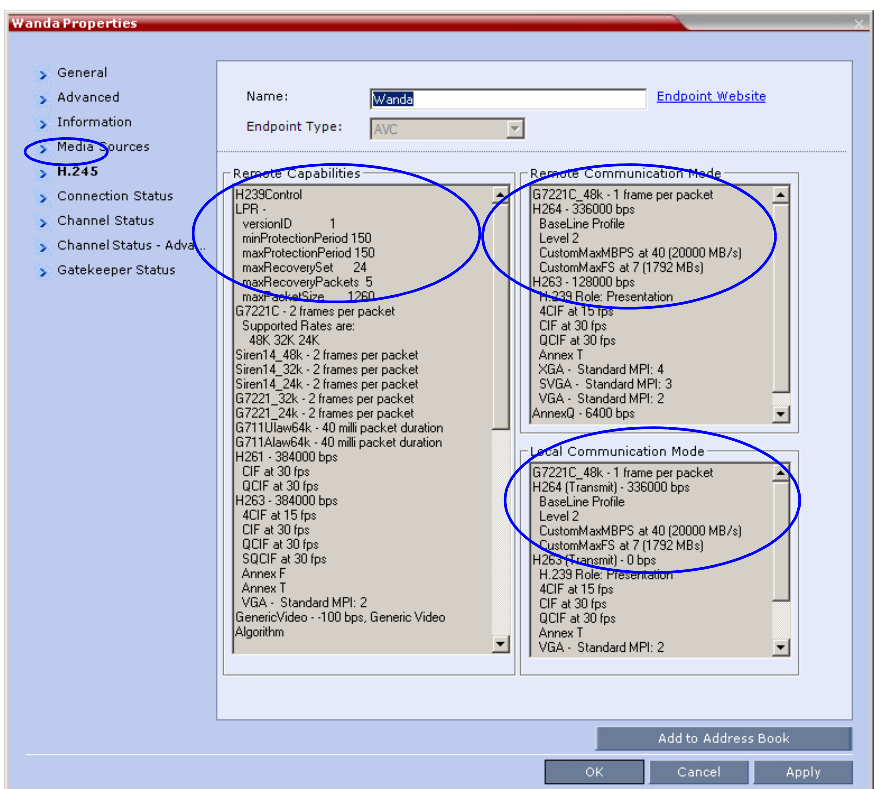
LPR is enabled or disabled in the *Conference Profile* dialog box.

- **CP Conferences –** *LPR* is enabled by default in the *New Profile – Advanced* dialog box.
- **VSW Conferences –** If *Video Switching* is selected, the LPR check box is automatically cleared and *LPR* is disabled. *LPR* can be enabled for VSW conferences but H.320 and SIP participants will not be able to connect.

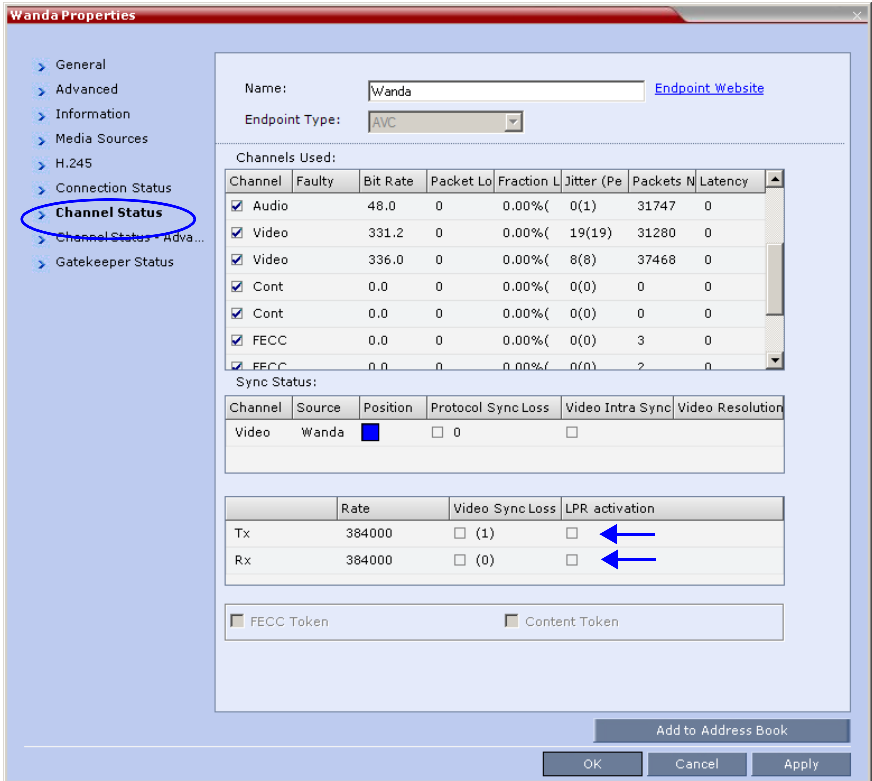
  For more information, see "*Defining New Profiles"* on page **2-18**.

Monitoring Lost Packet Recovery

In the *Participant Properties – H.245* tab, *LPR* activity is displayed in all three panes.

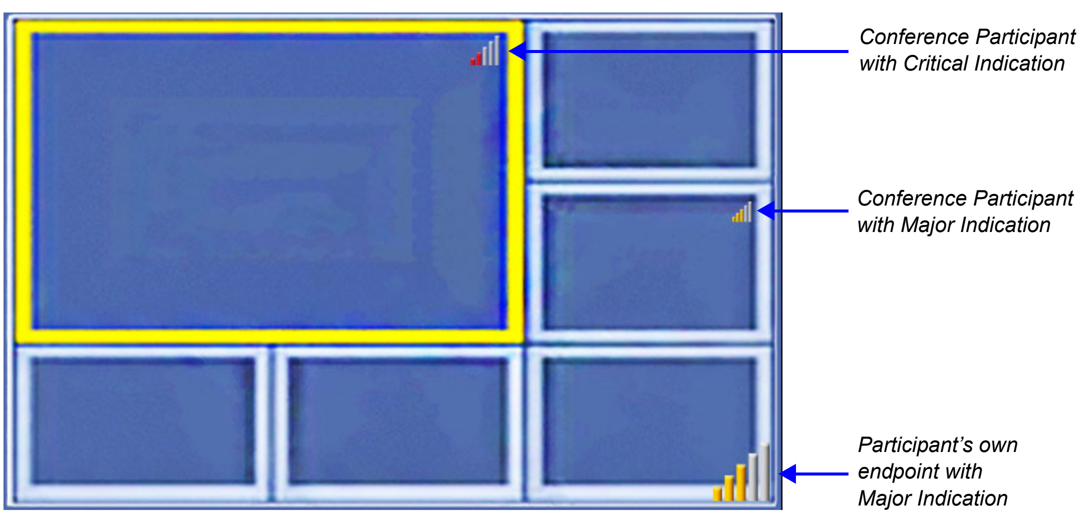


In the *Participant Properties – Channel Status* tab, check box indicators show *LPR* activation in the local and remote (transmit and receive) channels.



Network Quality Indication (AVC Only)

If network quality issues occur, *Network Quality Indicators* provide information to participants about their own network quality and that of other participants displayed in the cells of the conference *Video Layout*.



Guidelines

Network Quality Indicators are displayed for:

- The *Video Channel* only in *AVC Conferencing Mode*.
  Content, *Audio* and *FECC Channel* quality issues are not indicated.
- The participant's own endpoint:
  — *Network Quality Indicators* are displayed by default and can be disabled
  — For media transmitted to and received from the *RMX (Video in / Video out).*
- Participants displayed in the cells of the conference *Video Layout*:
  — *Network Quality Indicators* are not displayed by default and can be enabled
  — The media transmitted from the endpoint to the *RMX* (*Video in*).

Network Quality Indicators:

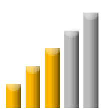
- Are supported with *MPMx* cards only
- Are not supported in:
  — *SVC Conferencing Mode*
  — *AVC - Video switched* conferences

Network Quality

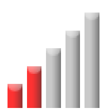
Network quality is determined by the percentage of packet loss according to the following default threshold values:

- Packet loss less than **1%** is considered *Normal*
- Packet loss in the range of **1% - 5%** is considered *Major*
- Packet loss above **5%** is considered *Critical*.

Major and *Critical* states are indicated with yellow and red indicator bars respectively.



Major



Critical

When network quality improves from *Critical* to *Major* remaining stable for 5 seconds, the *Network Quality Indicator* is changed accordingly and when network quality improves from *Major* to *Normal*, remaining stable for 5 seconds, the *Network Quality Indicator* is no longer displayed.

Indication Threshold Values

The default *Major* and *Critical* indication threshold values can be modified by manually adding the following *System Flags* and modifying their values as required.

Table 4-18 *Network Quality Indicator - Indication Threshold Flags*

Flag	Description
NETWORK_IND_MAJOR_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from *Normal* to *Major*. Default: 1

Table 4-18 Network Quality Indicator - Indication Threshold Flags (Continued)

Flag	Description
NETWORK_IND_CRITICAL_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from *Major* to *Critical*. Default: 5

For more information see "*Manually Adding and Deleting System Flags"* on page 22-18.

Customizing Network Quality Indicator Display

Display of the *Network Quality Indicators* can be customized for the following:

- The participant's own endpoint
- Participants displayed in the cells of the conference *Video Layout*

The *Network Quality Indicator* display can be customized by manually adding the following *System Flags* and modifying their values as required.

Table 4-19 Network Quality Indicator - Display Customization Flags

Flag	Description
DISABLE_SELF_NETWORK_IND	Disable the display of the *Network Quality Indicator* of the participant's own endpoint. Default: NO Range: YES / NO
DISABLE_CELLS_NETWORK_IND	Disable the display of *Network Quality Indicators* displayed in the cells of the conference *Video Layout*. Default: YES Range: YES / NO
SELF_IND_LOCATION	Change the location of the display of the *Network Quality Indicator* of the participant's own endpoint. Default: BOTTOM_RIGHT Range: • TOP_ LEFT • TOP • TOP_RIGHT • BOTTOM_ LEFT • BOTTOM • BOTTOM_RIGHT

Table 4-19 Network Quality Indicator - Display Customization Flags (Continued)

Flag	Description
CELL_IND_LOCATION	Change the location of the display of *Network Quality Indicators* displayed in the cells of the conference *Video Layout*. Default: TOP_RIGHT Range: • BOTTOM_LEFT • BOTTOM_RIGHT • TOP_LEFT • TOP_RIGHT

For more information see "*Manually Adding and Deleting System Flags"* on page **22-18**.

Telepresence Mode (AVC Only)

RMX supports the Telepresence Mode in *AVC Only* conferences allowing multiple participants to join a telepresence conference from RPX and TPX high definition rooms as well as traditional, standard definition video conferencing systems.

TPX (Telepresence) and RPX (Realpresence) room systems are configured with high definition cameras and displays that are set up to ensure that all participants share a sense of being in the same room.

Figure 4-1 Realpresence Participants using two RPX HD 400 Room Systems

The following are examples of situations where an RMX is needed for *Telepresence* configurations:

- RPX to TPX
- RPX 2-cameras/screens to RPX 4-cameras/screens
- 3 or more RPXs
- 3 or more TPXs

RMX Telepresence Mode Guidelines

System Level

- The RMX system must be licensed for *Telepresence Mode.*
- The system must be activated with a *Telepresence* enabled license key.

Conference Level

- The *Telepresence Mode* and *Telepresence Layout Mode* fields are only displayed in the Conference Profile dialog box if the RMX has a Telepresence license installed.
- A *Telepresence* conference must have *Telepresence Mode* enabled in its profile.
- In *Telepresence Mode*, ITP sites are automatically detected.
- When Telepresence mode is selected in a conference profile, the following options are disabled:
  - — borders
  - — site names
  - — speaker indication
  - — skins
  - — same layout
  - — presentation mode
  - — auto layout
  - — lecture mode
- The master (center) camera is used for video, audio and content.
- *Conference Templates* can be used to simplify the setting up *Telepresence* conferences where precise participant layout and video forcing settings are crucial. *Conference Templates:*
  - — Save the conference Profile.
  - — Save all participant parameters including their *Personal Layout* and *Video Forcing* settings.
- An ongoing *Telepresence* conference can be saved to a *Conference Template* for later re-use.

  For more information see "*Conference Templates"* on page **11-1**.

Room (Participant/Endpoint) Level

- To the RMX, each camera in a *Telepresence* room is considered to be an endpoint and is configured as a participant.
- The *Telepresence Mode* field is always displayed in the *New Participant* dialog box. If the system is not licensed for *Telepresence* this field is automatically set to None.
- *Telepresence* participants (endpoints) must be specified as:
  - — RPX – transmitting 4:3 video

    or
  - — TPX – transmitting 16:9 video

Automatic Detection of Immersive Telepresence (ITP) Sites

When the conference *Telepresence Mode* is set to Auto (Default) *ITP* endpoints are automatically detected.

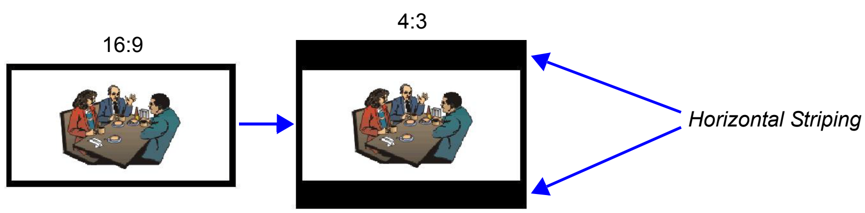
If an *ITP* endpoint is detected in such conference, *ITP* features are applied to **all** endpoints and the RMX sends conference video with the following options disabled:

- Borders
- Site names
- Speaker indication
- Skins
- Same Layout
- Presentation Mode
- Auto Layout
- Lecture Mode

The ITP features are dynamic, and if all ITP endpoints disconnect from the conference, normal conference video is resumed for the remaining all participants. ITP features are re-applied to all participants should an ITP endpoint re-connects to that conference.

Horizontal Striping

Horizontal Striping is used by the RMX in order to prevent cropping and preserve the aspect ratio of video for all *Telepresence Modes*.

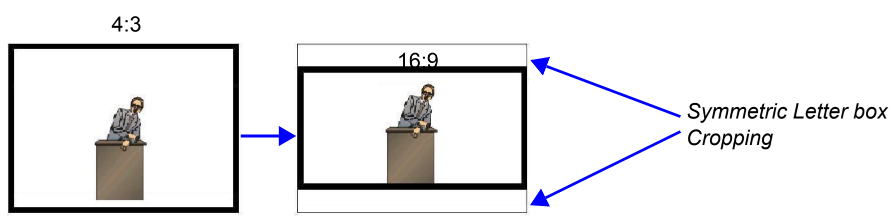


Cropping

Cropping is used by the RMX in order to preserve the aspect ratio of video for all *Telepresence Modes*.

Cropping is controlled by the **ITP_CROPPING** system flag in the system configuration, providing different cropping options according to the endpoints participating in the Telepresence conference.

By default, the flag is set to **ITP**. In this mode, the area to be stripped is cropped equally from the top and the bottom (as shown in the example below). For more details, see "*Modifying System Flags"* on page **22-1**.



Video Fade in Telepresence conferences

Video Fade is enabled for all *Telepresence* conferences.

Gathering Phase with ITP Room Systems

When a conference is configured to include a *Gathering Phase*, only one endpoint name is displayed for the *ITP* room in the connected participant list of the *Gathering* slide. The *ITP* room endpoint with the suffix “1” in its name receives the *Gathering* slide.

Aspect ratio for standard endpoints

Standard endpoints (non-*ITP*) receive video from the RMX with the same aspect ratio as that which they transmitted to the RMX.

Skins and Frames

When Telepresence Mode is enabled, no Skin is displayed and the system uses a black background. Frames around individual layout windows and the speaker indication are disabled.

RPX and TPX Video Layouts

Additional video layouts have been created to give *Telepresence* operators more video layout options when configuring TPX and RPX room systems. These additional video layout options are available to all endpoints on both conference layout and *Personal Layout* levels.

***Table 4-20** TPX / RPX – Additional Video Layouts*

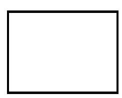
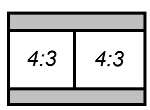
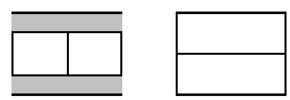
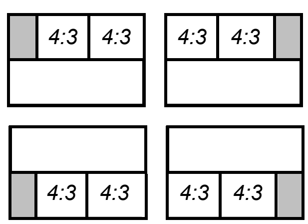
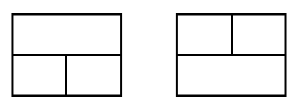
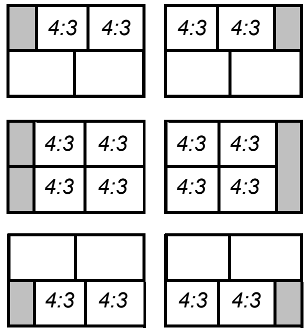
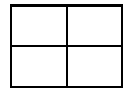
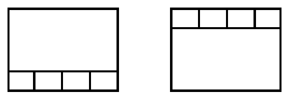
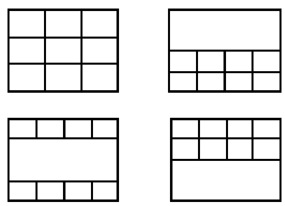
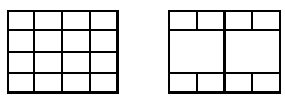
Number of Endpoints	Layouts	
1		
2		
3		

Table 4-20 TPX / RPX – Additional Video Layouts (Continued)

Number of Endpoints	Layouts	
4		
5		
9		
10+		

The following example illustrates the use of standard and additional RMX *Telepresence* layouts when connecting four Room Systems as follows:

- Two TPX Room Systems
  - — 2 active cameras
  - — 6 screens
- Two RPX Room Systems
  - — 8 cameras
  - — 8 screens

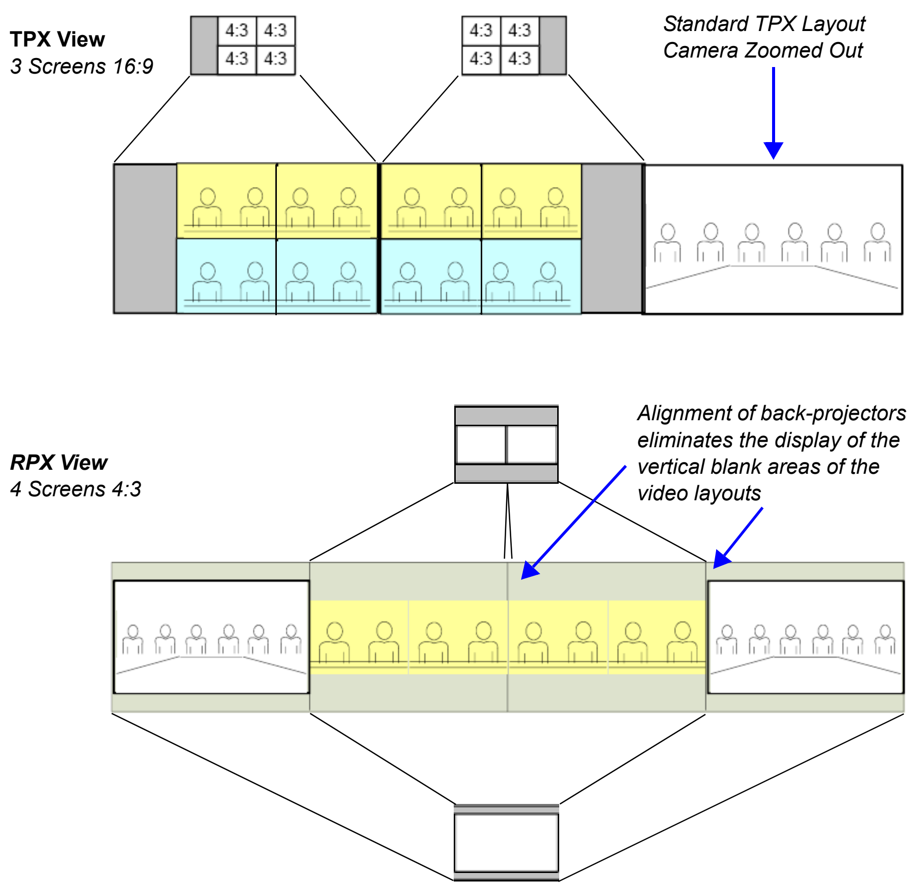


Figure 4-2 *RPX and TPX Room System connected using the RMX 1500/2000/4000*

Enabling Telepresence Mode

Conference Level

Telepresence Mode must be configured in a new or existing Conference Profile.

To enable Telepresence in a new or existing Conference Profile:

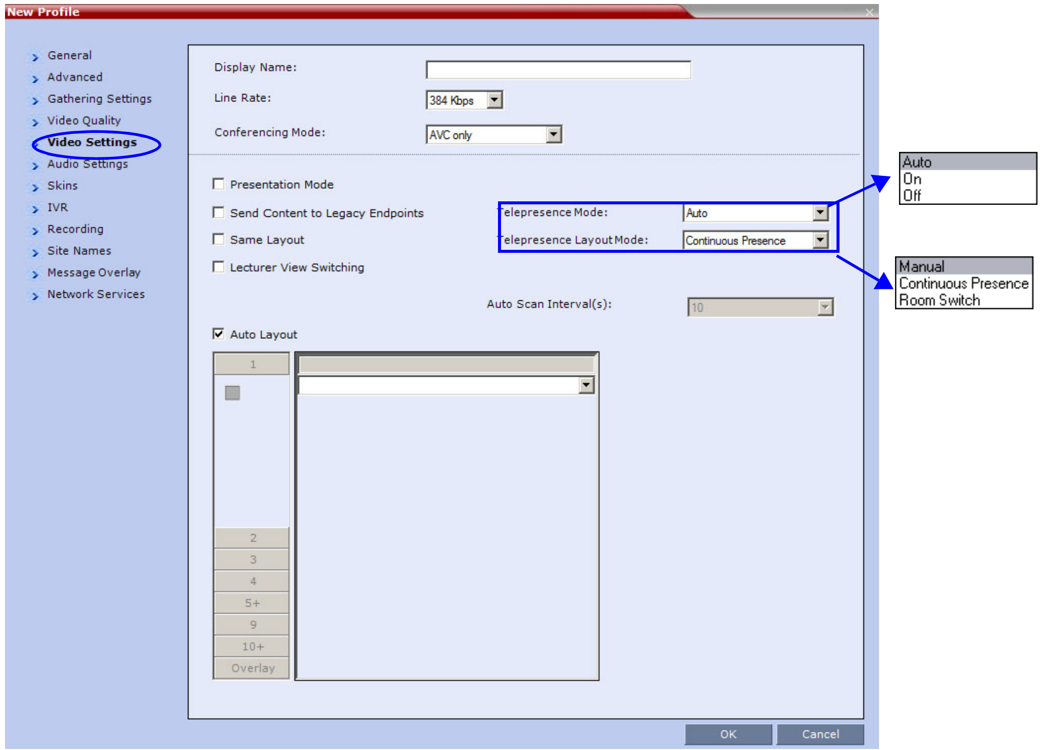
1 In the *RMX Management* pane, click **Conference Profiles**.

2 Click the **New Profiles** ( ) button or open an existing *Conference Profile*.

3 Define the various profile *General*, *Advanced*, *Gathering Settings* and *Video Quality* parameters.

For more information on defining Profiles, see "*Defining New Profiles"* on page **2-18**.

4 Click the **Video Settings** tab.



5 In the *Telepresence Mode* field, select one of the following options:

— **OFF** - When OFF is selected, normal conference video is sent by the RMX.

— **AUTO (Default) -** The ITP features are dynamic. When AUTO is selected and an ITP endpoint is detected, ITP features are applied to the conference video for all participants. If all ITP endpoints disconnect from the conference, normal conference video is resumed for all remaining participants. ITP features are re-applied for all participants should an ITP endpoint re-connect to the conference.

— **ON** - ITP features are always applied to the conference video for all participants regardless of whether there are ITP endpoints connected or not.

6 In the *Telepresence Layout Mode* field, select the Telepresence Layout Mode to be used in the conference. This field is used by VNOC operators and Polycom Multi Layout Applications to retrieve Telepresence Layout Mode information from the RMX.

The following modes can be selected (as required by the VNOC and Polycom Multi Layout Applications):

— **Manual**

— **Continuous presence - Room Continuous Presence (Default)**

— **Room Switch - Voice Activated Room Switching**

7 Select the required video layout.

> When Telepresence Mode is enabled, the Skin options are disabled as the system uses a black background and the frames and speaker indication are disabled.

8 Click **OK**.

Multiple Cascade Links

Multiple Cascade Links enable *Cascading* between RMXs hosting conferences that include *Immersive Telepresence Rooms* (*ITP*) such as Polycom’s OTX and RPX Room Systems.

In previous versions the video stream of only one of the *ITP* endpoints could be sent to the remote RMX.

Guidelines

- *Multiple Cascade Links* are implemented by creating a *Link Participant* which consists of a main link and sub-links which are automatically generated and sequentially numbered. For more information see "*Creating a Link Participant” on page* **4-66**.
- All cascaded links must use H.323 protocol.
- *Multiple Cascade Links* are supported with *MPMx* and *MPM*+ cards.
- *Multiple Cascade Links* are supported in *CP* conferencing mode.
- The number of cascading links is defined manually according to the maximum number of Room System cameras in the cascaded conference.
- When the active speaker is in an Immersive Telepresence Room, *Multiple Cascade Links* are used, one link for each of the Room System’s cameras.
  — An RPX 4xx Room System requires 4 *Cascaded Links* to carry the video of its 4 cameras.
  — An RPX 2xx Room System requires 2 *Cascaded Links* to carry the video of its 2 cameras.
  — An OTX 3xx Room System requires 3 *Cascaded Links* to carry the video of its 3 cameras. The OTX Room System must be configured as *Room Switch* in order to send multiple streams. When configured in *CP Mode*, its cameras zoom out and all 3 screens are sent as one stream.
- The number of links is defined when creating the *Link Participant*. Each conference in the cascade must have a *Link Participant* with the same number of *Multiple Cascade Links* defined. Calls from *Link Participants* not defined with the same number of links are rejected. *Number of cascading links is not identical for all conferences* is listed as the *Call Disconnection Cause*. For more information see "*Creating a Link Participant”* on page **4-66** and "*Monitoring Multiple Cascade Links”* on page **1-1**.
- Although it is possible to disconnect and reconnect specific *Multiple Cascade Links* using the *RMX Web Client* / *RMX Manager* it not advisable to do so.

— If the main link is disconnected all sub-links are disconnected and deleted. Reconnecting the main link reconnects all sub-links.

— If a sub-link is disconnected it remains disconnected until it is manually reconnected.

— The number of *Multiple Cascade Links* cannot be modified while any of the links are in a disconnected state. All previous links must be deleted before modification is possible.

For more information see "*Monitoring Multiple Cascade Links"* on page **1-1**.

- A *Link Participant* can be dragged from the address book into a conference.
  — If it is the first *Link Participant* in the conference, the number of *Multiple Cascade Links* defined for the participant are created and connected.
  — If it is not the first *Link Participant* in the conference, the number of *Multiple Cascade Links* defined for the participant is ignored.
- If there are insufficient resources to connect all *Multiple Cascade Links* in either of the RMXs, none of the links are connected and *resources deficiency -0* is listed as the *Call Disconnection Cause*. For more information see "*Monitoring Multiple Cascade Links"* on page **1-1**.
- *Multiple Cascade Links* that are not used by MLA are inactive but continue to consume resources.
- All RMXs participating in the cascade must have the same *Telepresence Mode* definitions, either all defined as *CP* or all defined as *Room Switch*.
- When *Multiple Cascade Links* are defined in the *Conference Profile*, the *Layout Type* field of the *Link Participant*'s *Participant Properties - Media Sources* dialog box is set to **Conference** and cannot be modified.
- TIP Telepresence Rooms (CTS) are supported without *Content.* For more information see "*Collaboration With Cisco's Telepresence Interoperability Protocol (TIP)"* on page **I-1**.

Enabling and Using Multiple Cascade Links

The settings required to enable *Multiple Cascade Links* on the RMX are minimal and are described in "*Creating a Link Participant"* on page **4-66**.

Most of the layout configuration is performed using *Polycom's Multipoint Layout Application (MLA)*.

Figure 4-3 and Figure 4-4 show example layouts and media flows when MLA is configured for a cascading conference between two RMXs.

In Figure 4-3:

- The OTX Room System connects to RMX A.
- The RPX Room System connects to RMX B.
- This layout requires that the *Telepresence Layout Mode* to be set to **Room Switch** in the *Conference Profiles* of the *Cascading Conferences* in each RMX.
- The current speaker is a participant in the RPX ITP Room.

- Directional media flows, A ⇆ B, are shown separately for readability purposes.

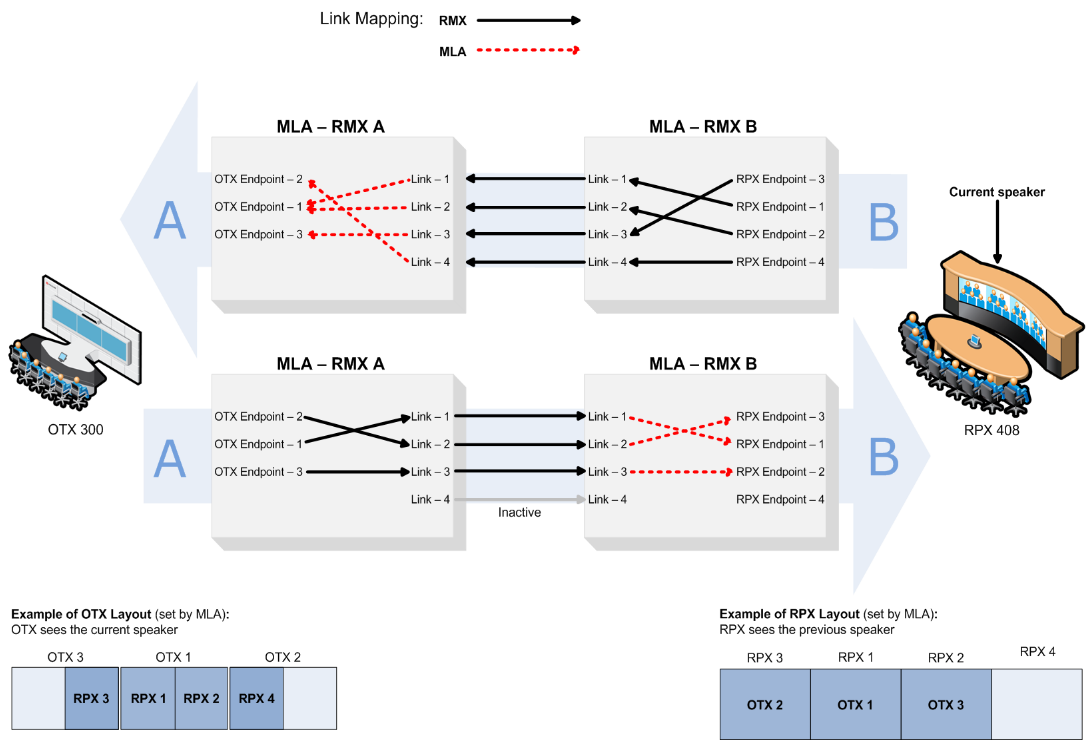


Figure 4-3 *RMX Telepresence Layout Mode - Room Switch*

In Figure 4-4:

- An HDX endpoint and an OTX Room System connects to RMX A.
- An HDX endpoint and an RPX Room System connects to RMX B.
- This layout requires that the *Telepresence Layout Mode* to be set to **Continuous Presence** in the *Conference Profiles* of the *Cascading Conferences* in each RMX.

- The current speaker is the HDX endpoint connected to RMX A.

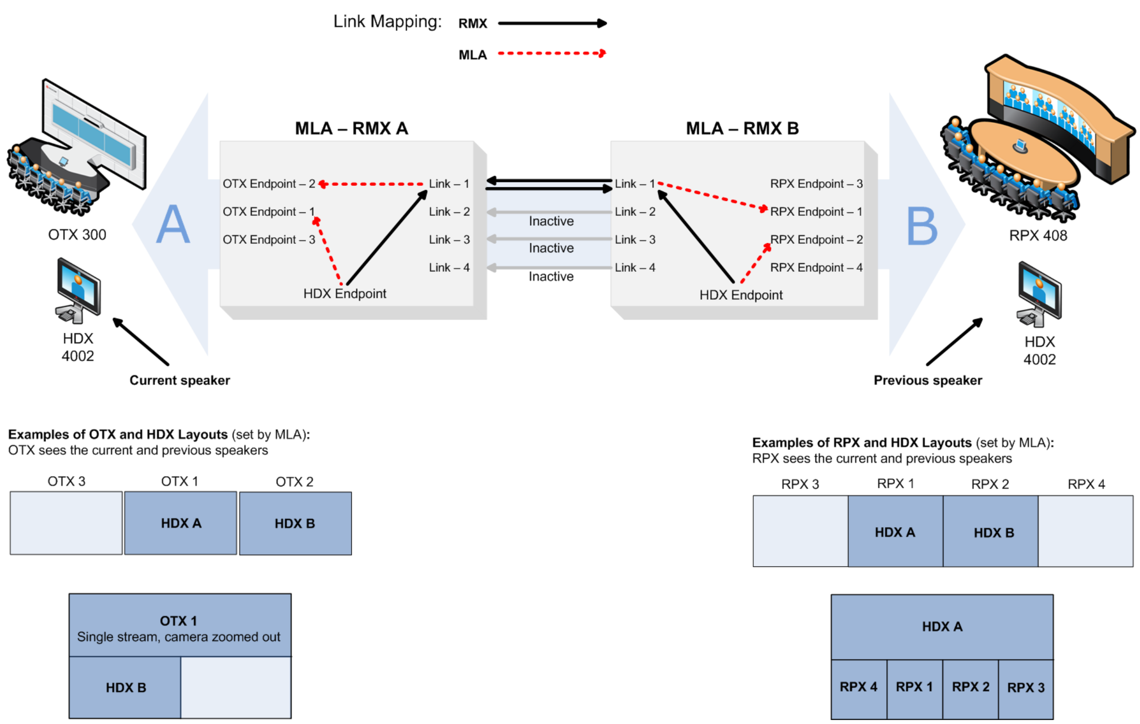


Figure 4-4 *RMX Telepresence Layout Mode - Continuous Presence*

For more information see:

- *"Telepresence Layout Mode" on page* 2-33.
- *Polycom® Multipoint Layout Application (MLA) User's Guide for Use with Polycom Telepresence Solutions*
- *Polycom® Immersive Telepresence (ITP) Deployment Guide*

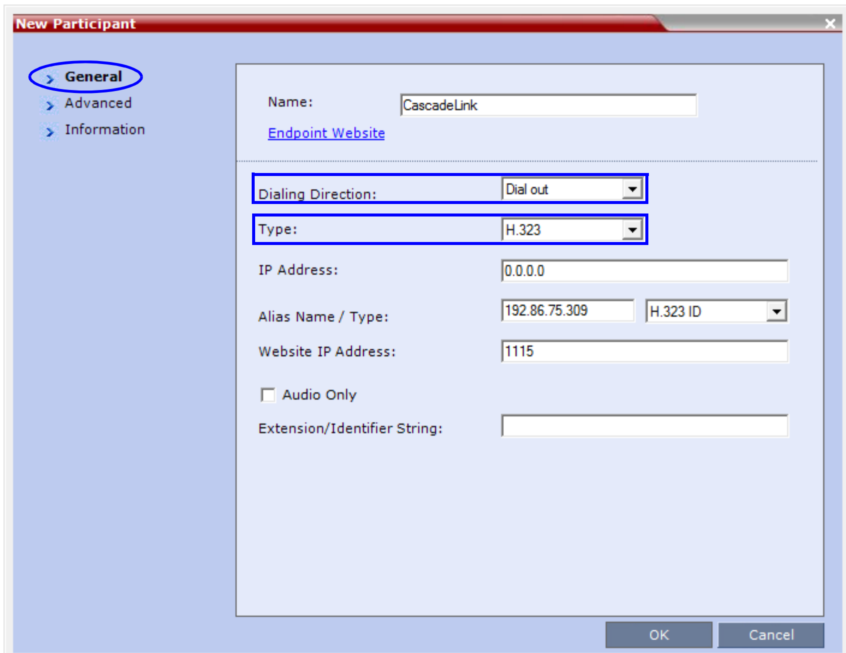
Creating a Link Participant

Link Participant in the Dial Out RMX

The *Link Participant* is defined in the *New Participant* dialog box.

In the *General* tab:

- *Dialing Direction* must be selected as **Dial out.**
- *Type* must be selected as **H.323**.



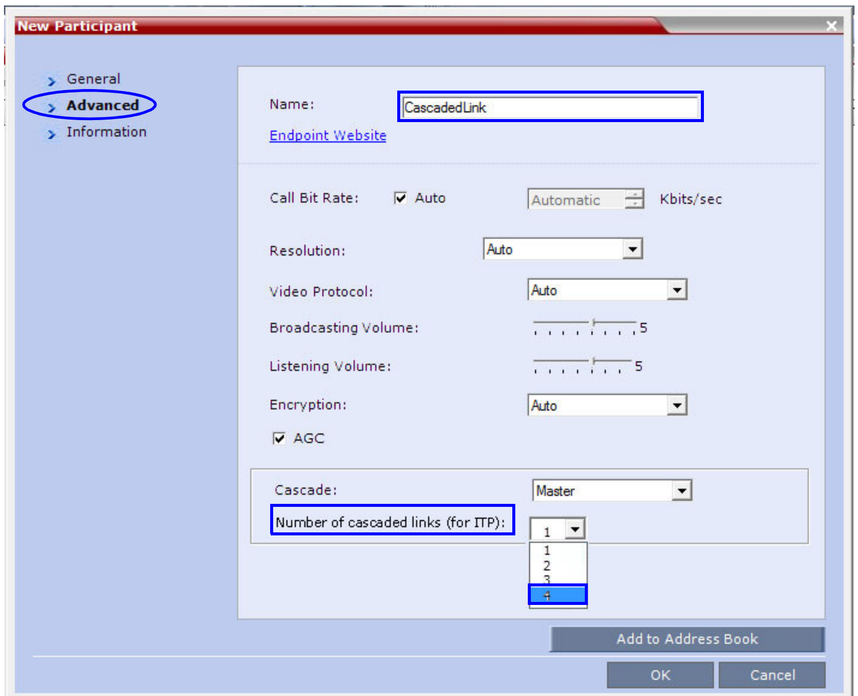
For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide, "Creating a Cascade Enabled Dial-out/Dial-in Participant Link"* on page **5-15**.

In the *Advanced* tab:

(This field is only enabled if the RMX system is licensed for *Telepresence Mode*.)

- In the *Cascade* drop-down menu, select either **Master** or **Slave**.
- In the *Number of cascaded links (for ITP)* drop-down menu, select the maximum number of *Multiple Cascade Links* required according to the number of Room System endpoints in the cascaded conference.

  For example if an *RPX 4xx* is included, the number of links required is 4.



The RMX automatically adds a number suffix to the name of the *Link Participant*, for example if the *Participant Link Name* is *CascadeLink* and the *Number of cascaded links (for ITP)* field is set to 4, the following *Multiple Cascade Links* are created:

- *CascadeLink-1*
- *CascadeLink-2*
- *CascadeLink-3*
- *CascadeLink-4*

Participant Link in the Dial In RMX

The call from *Participant Link* defined in the *Dial-out* RMX in identified by the *Dial-in* RMX as having been initiated by a *Participant Link*.

Suffixes are appended the *Multiple Cascade Links* according to the *Number of cascaded links (for ITP)* field depending on whether the *Dial -In Participant Link* is defined or un-defined:

Participant Link is an un-defined:

The *Multiple Cascade Link* names are automatically assigned by the RMX.
For example on a RMX 1500 the names of the links are:

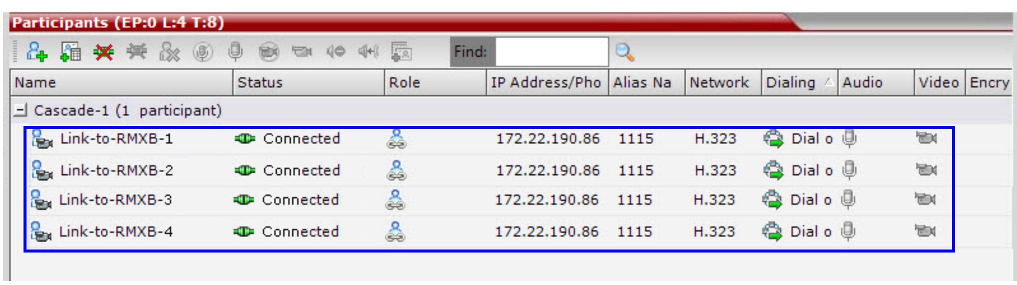
- *POLYCOM RMX 1500-1,*
- *POLYCOM RMX 1500-2*
- *POLYCOM RMX 1500-3, etc.*

Participant Link is a defined:

The *Multiple Cascade Link* names are assigned according to the name of the defined participant that is to function as the cascade link and the *Number of cascaded links (for ITP)* information sent by the calling *Dial-Out Participant Link*.
For example if the defined participant that is to function as the cascade link is named *Cascade_Link_From_B* the names of the links are:

- *Cascade_Link_From_B-1*
- *Cascade_Link_From_B-2*
- *Cascade_Link_From_B-3, etc.*

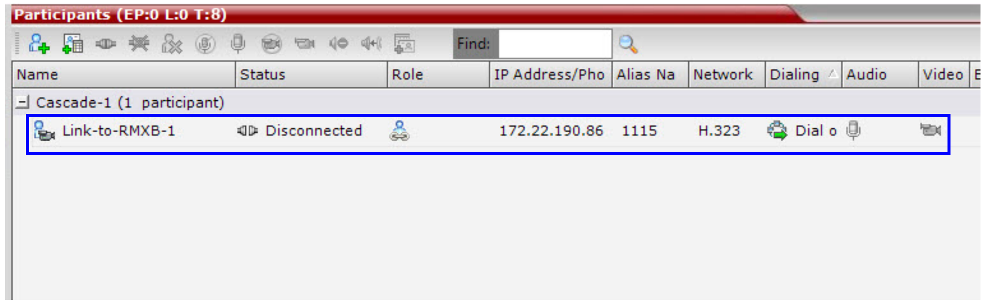
Multiple Cascade Links connections can be monitored in the *Participants* list of the *RMX Web Client / RMX Manager* main screen:



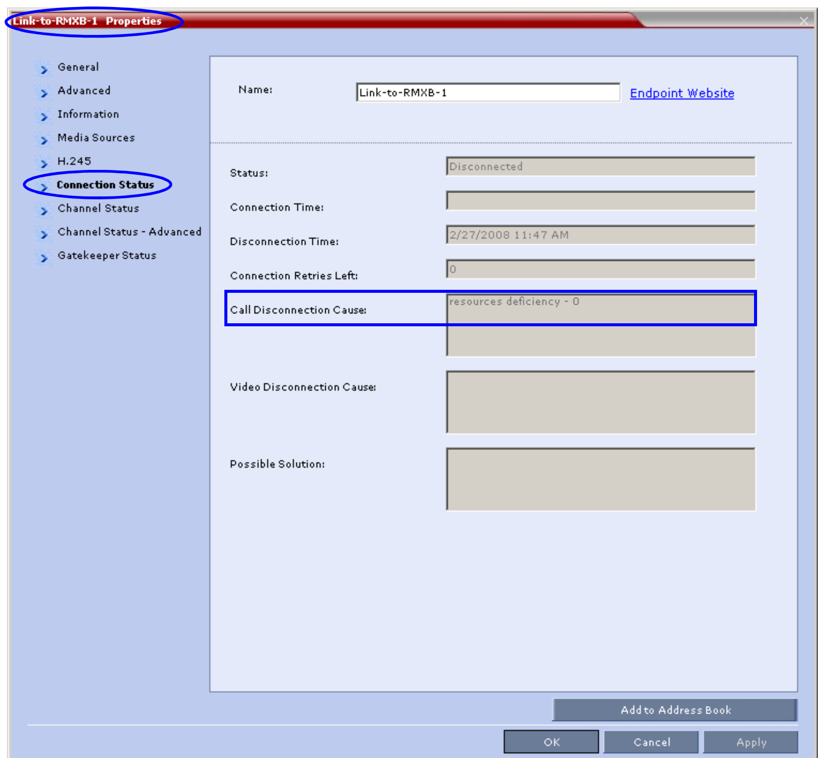
Disconnection Causes

- If there are insufficient resources to connect all the required links:
  - None of the links are connected.

— The first link is listed as **Disconnected** in the *Participants* list of the *RMX Web Client / RMX Manager* main screen.



— Resource deficiency is listed as the *Call Disconnection Cause* in the *Participant Properties - Connection Status* dialog box.

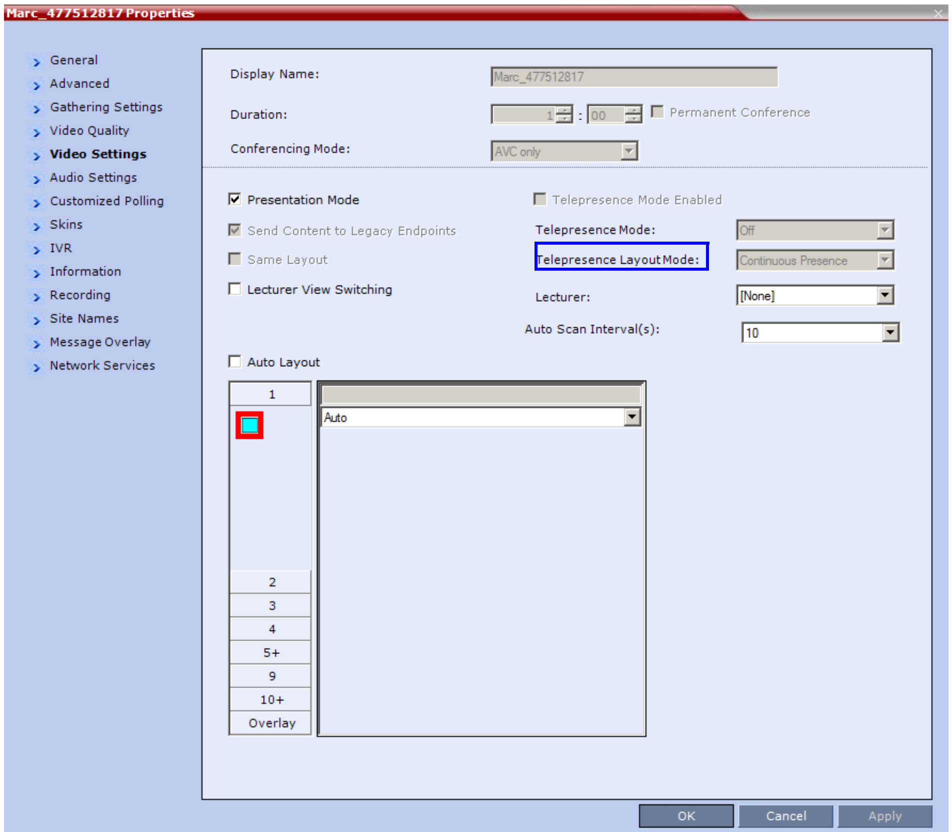


- If a calling *Link Participant* is not defined with same number of links as all the other *Link Participants* in the cascaded conferences:
  — The call is rejected.
  — The *Call Disconnection Cause* is: *Number of cascading links is not identical for all conferences.*

Monitoring Telepresence Mode

Monitoring Ongoing Conferences

An additional status indicator, *Telepresence Mode Enabled*, is displayed in the *Conference Properties - Video Settings* tab when monitoring ongoing conferences.

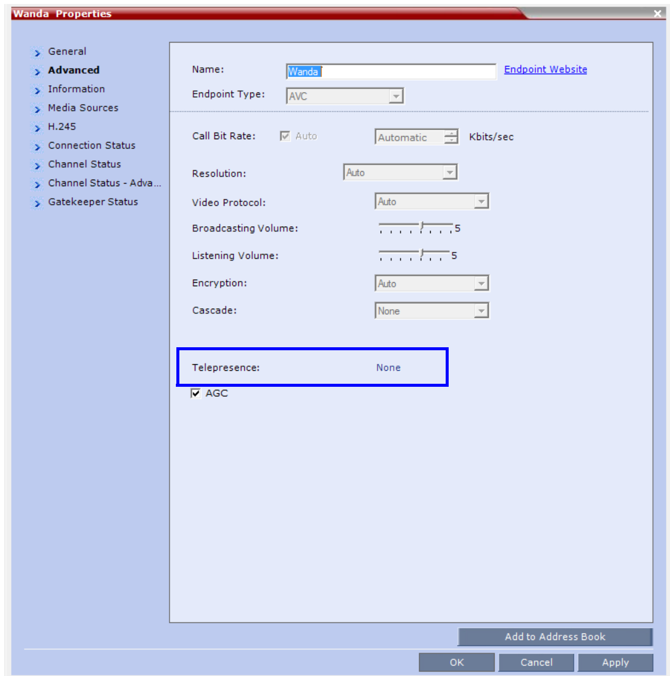


The *Telepresence Mode Enabled*, *Telepresence Mode* and *Telepresence Layout Mode* fields are only enabled if the RMX has a *Telepresence* license installed.

If *Telepresence Mode* is enabled, a check mark is displayed in the check box. This option is grayed as this is a status indicator and cannot be used to enable or disable *Telepresence Mode*.

Monitoring Participant Properties

An additional status indicator, *Telepresence*, is displayed in the *Participant Properties - Advanced* tab when monitoring conference participants.

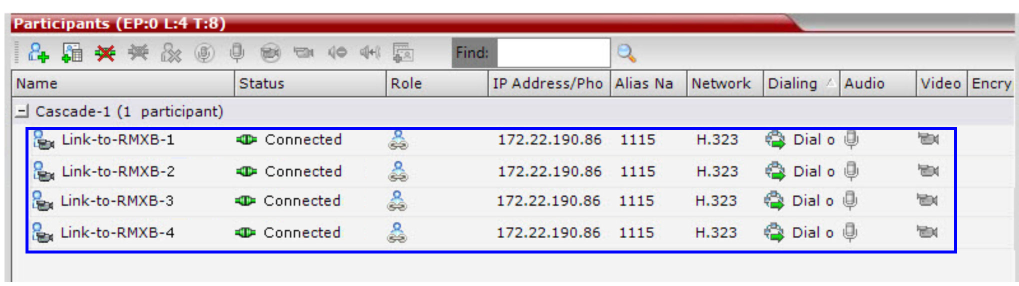


The *Telepresence* mode of the participant is indicated:

- *RPX* - the participant's endpoint is transmitting 4:3 video format.
- *TPX* - the participant's endpoint is transmitting 16:9 video format.
- *None*.

Monitoring Multiple Cascade Links

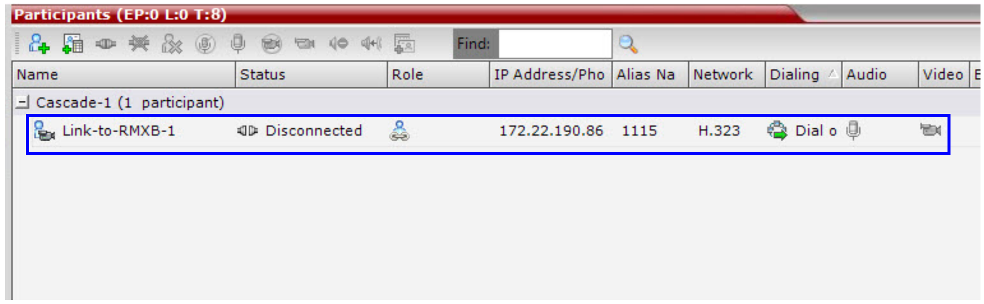
Multiple Cascade Links connections can be monitored in the *Participants* list of the *RMX Web Client / RMX Manager* main screen:



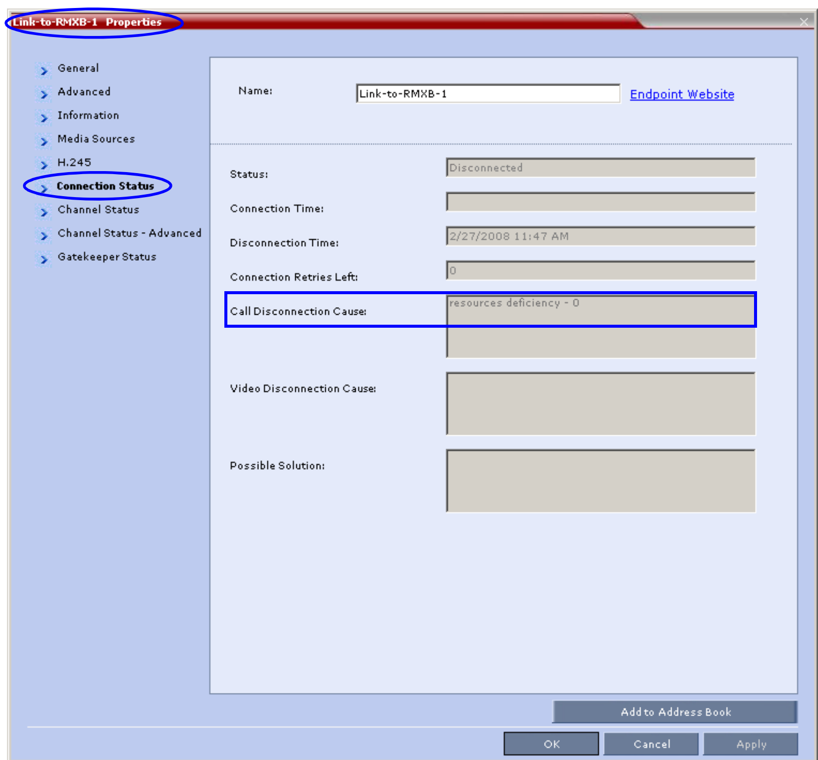
Disconnection Causes

- If there are insufficient resources to connect all the required links:
  — None of the links are connected.

— The first link is listed as **Disconnected** in the *Participants* list of the *RMX Web Client / RMX Manager* main screen.



— Resource deficiency is listed as the *Call Disconnection Cause* in the *Participant Properties - Connection Status* dialog box.



- If a calling *Link Participant* is not defined with same number of links as all the other *Link Participants* in the cascaded conferences:
  — The call is rejected.
  — The *Call Disconnection Cause* is: *Number of cascading links is not identical for all conferences.*

Lecture Mode (AVC Only)

Lecture Mode enables all participants to view the lecturer in full screen while the conference lecturer sees all the other conference participants in the selected layout while he/she is speaking. When the number of sites/endpoints exceeds the number of video windows in the layout, switching between participants occurs every 15 seconds. Conference participants cannot change their Personal Layouts while Lecture Mode is enabled.

Automatic switching is suspended when one of the participants begins talking, and it is resumed automatically when the lecturer resumes talking.

Lecture Mode is available only in *AVC Conferencing Mode.*

Enabling Lecture Mode

Lecture Mode is enabled at the conference level by selecting the lecturer. Conference participants cannot change their Personal Layouts while Lecture Mode is enabled.

Automatic switching between participants viewed on the lecturer's screen is enabled in the conference Profile.

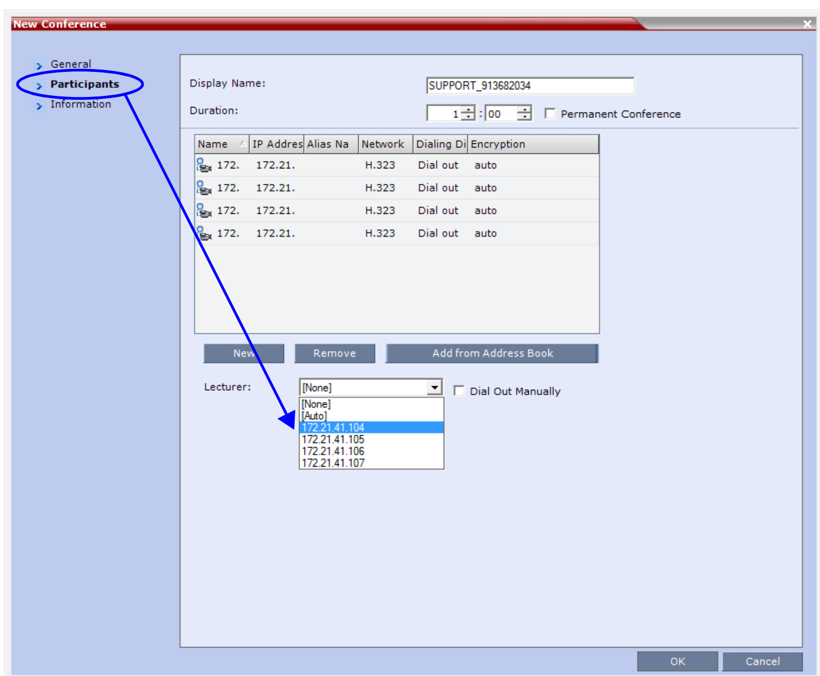
Selecting the Conference Lecturer

Selecting a lecturer for the ongoing conference, enables the Lecture Mode. You can select the lecturer:

- during the definition of the ongoing conference
- after the conference has started and the participants have connected to the conference.

To select the lecturer and enable the Lecture Mode while starting the conference:

>> In the *Conference Properties - Participant* dialog box, enable the Lecture Mode in one of the following methods:



Selecting a defined participant:

a Add participants to the conference either from the Address book or by defining new participants.

b In the **Lecturer** field, select the lecturer from the list of the defined participants.

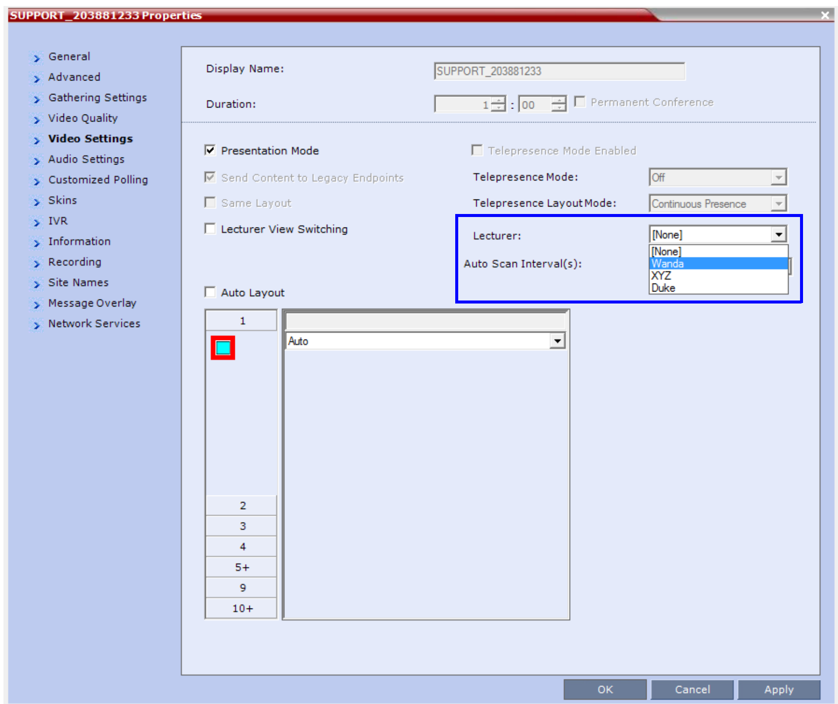
Automatic selection of the lecturer:

— In the **Lecturer** field, select **[Auto]**.
In this mode, the conference speaker becomes the lecturer.

To select the lecturer and enable the Lecture Mode during the ongoing conference:

1 Make sure that the participant you want to designate as the lecturer has connected to the conference.

2 In the *Conference Properties - Video Settings* dialog box, in the **Lecturer** field, select the lecturer from the list of the connected participants.

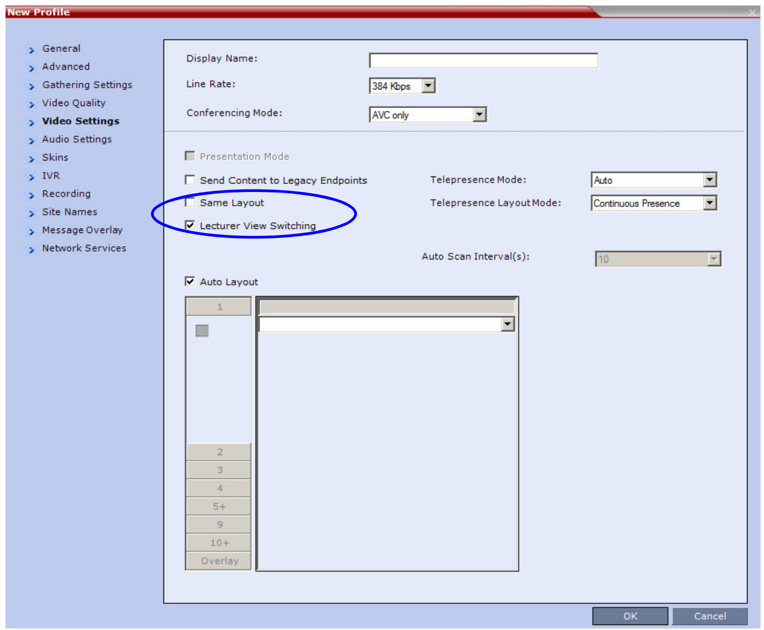


Defined dial out participants and dial in participants are considered to be two separate participants even if they have the same IP address/number. Therefore, if a defined dial-out participant is added to the conference and the same participant then dials in (before the system dialed out to that participant) the system creates a second participant in the Participants list and tries to call the dial-out participant. If the dial-out participant was designated as the conference lecturer, the system will not be able to replace that participant with the dial-in participant that is connected to the conference.

Enabling the Automatic Switching

Automatic switching between participants viewed on the lecturer's screen is enabled in the conference Profile, or during the ongoing conference, in the Conference Properties.

>> In the *Profile Properties - Video Settings* dialog box, select the **Lecturer View Switching** check box.



This option is activated when the conference includes more sites than windows in the selected layout. If this option is disabled, the participants will be displayed in the selected video layout without switching.

For more information about Profile definition, see "*Defining a CP Conference Profile"* on page **2-11**.

>> Once the conference is running, in the *Conference Properties - Video Settings* dialog box, select the **Lecturer View Switching** check box.

Lecture Mode Monitoring

A conference in which the Lecture Mode is enabled is started as any other conference. The conference runs as an audio activated Continuous Presence conference until the lecturer connects to the conference. The selected video layout is the one that is activated when the conference starts. Once the lecturer is connected, the conference switches to the Lecture Mode.

When *Lecturer View Switching* is activated, it enables automatic switching between the conference participants in the lecturer's video window. The switching in this mode is not determined by voice activation and is initiated when the number of participants exceeds the number of windows in the selected video layout. In this case, when the switching is performed, the system refreshes the display and replaces the last active speaker with the current speaker.

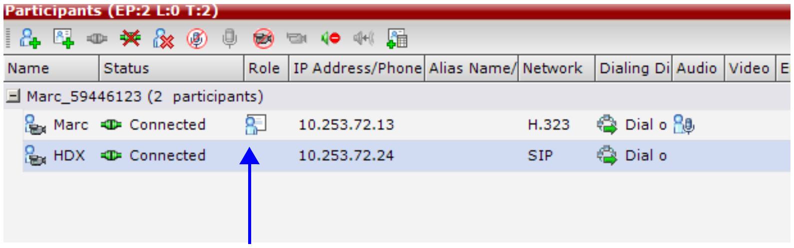
When one of the participants is talking, the automatic switching is suspended, showing the current speaker, and it is resumed when the lecturer resumes talking.

If the lecturer is disconnected during an Ongoing Conference, the conference resumes standard conferencing.

Forcing is enabled at the Conference level only. It applies only to the video layout viewed by the lecturer as all the other conference participants see only the lecturer in full screen.

If an asymmetrical video layout is selected for the lecturer (i.e. 3+1, 4+1, 8+1), each video window contains a different participant (i.e. one cannot be forced to a large frame and to a small frame simultaneously).

When *Lecture Mode* is enabled for the conference, the lecturer is indicated by an icon ( ) in the *Role* column of the *Participants* list.

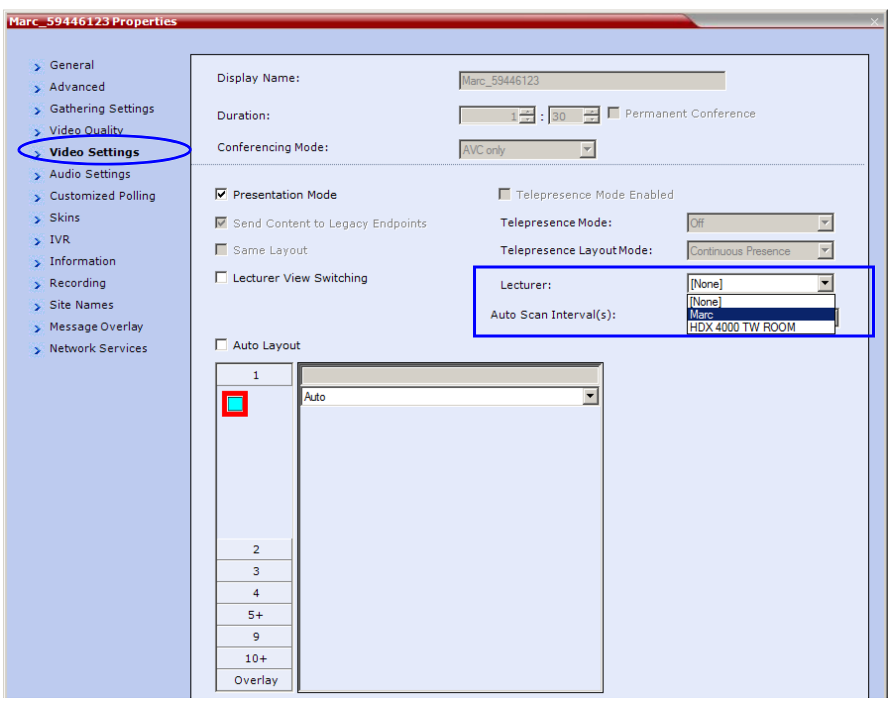


Participant designated as the Lecturer

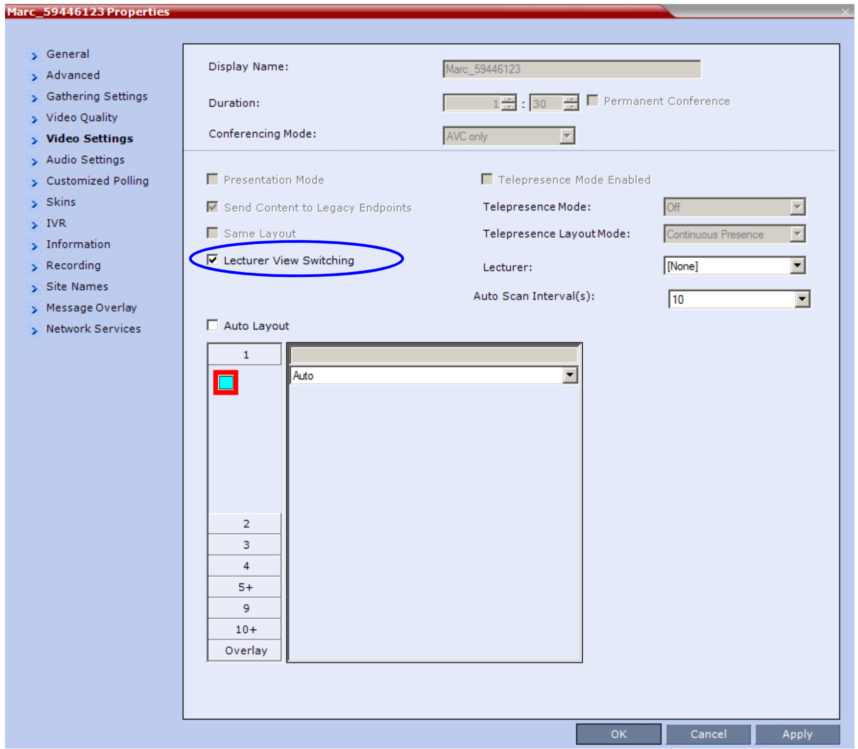
To control the Lecture Mode during an Ongoing Conference:

During the Ongoing Conference, in the *Conference Properties - Video Settings* dialog box you can:

- Enable or disable the Lecture Mode and designate the conference lecturer in the *Lecturer* list; select **None** to disable the Lecture Mode or select a participant to become the lecturer to enable it.
- Designate a new lecturer.



- Enable or disable the *Lecturer View Switching* between participants displayed on the lecturer monitor by selecting or clearing the **Lecturer View Switching** check box.



- Change the video layout for the lecturer by selecting another video layout.

Restricting Content Broadcast to Lecturer

Content broadcasting can be restricted to the conference lecturer only, when one of the conference participants is set as the lecturer (and not automatically selected by the system). Restricting the Content Broadcast prevents the accidental interruption or termination of H.239 Content that is being shared in a conference.

Content Broadcast restriction is enabled by setting the **RESTRICT_CONTENT_BROADCAST_TO_LECTURER** *system flag* to **ON**. When set to OFF (default) it enables all users to send Content.

When enabled, the following rules apply:

- Content can only be sent by the designated lecturer. When any other participant tries to send Content, the request is rejected.
- If the RMX user changes the designated lecturer (in the *Conference Properties - Video Settings* dialog box), the Content of the current lecturer is stopped immediately and cannot be renewed.
- The RMX User can abort the H.239 Session of the lecturer.
- Content Broadcasting is not implemented in conferences that do not include a designated lecturer and the lecturer is automatically selected by the system (for example, in *Presentation Mode*).

Muting Participants Except the Lecturer

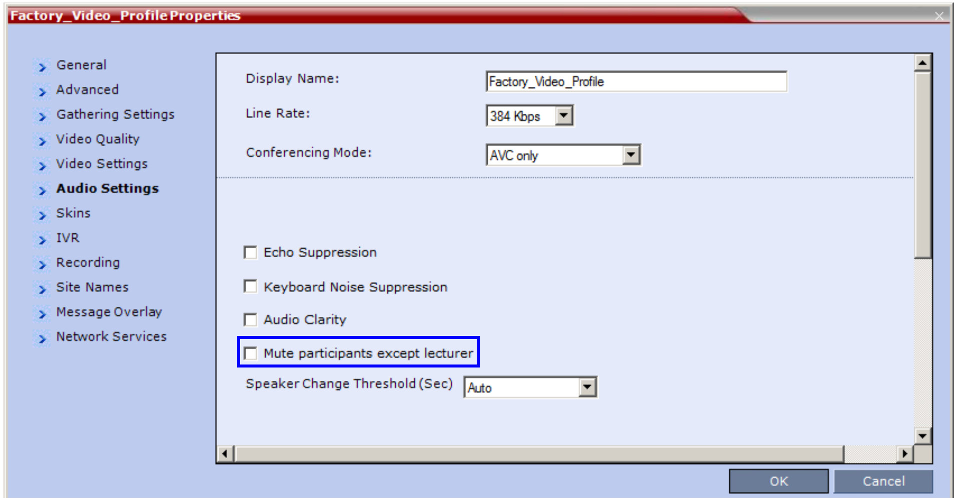
When the *Mute Participants Except Lecturer* option in the *Conference Profile* is enabled*,* the audio of all participants in the conference except for the lecturer can be automatically muted upon connection to the conference. This prevents other conference participants from accidentally interrupting the lecture, or from a noisy participant affecting the audio quality of the entire conference. Muted participants cannot unmute themselves unless they are unmuted from the RMX Web Client/RMX Manager.

Guidelines

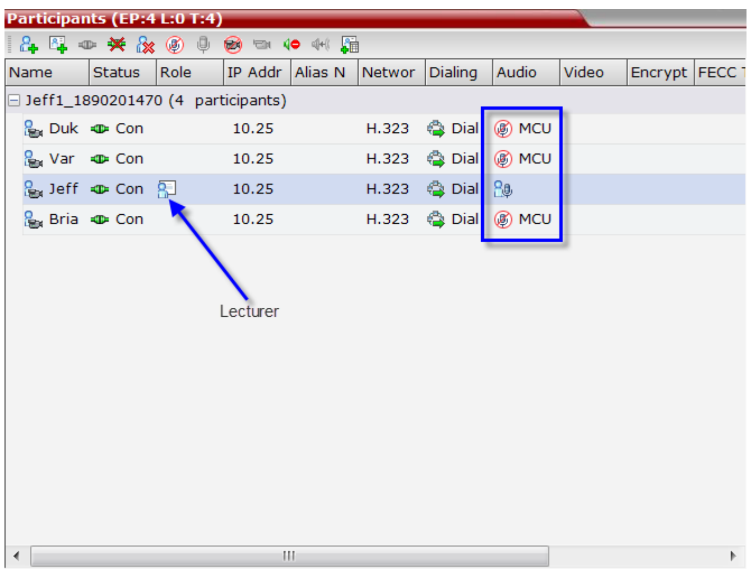
- Both Administrators and Operators (users) are allowed to set the *Mute Participants Except Lecturer* option.
- When the *Mute Participants Except Lecturer* option is enabled, the mute indicator on the participant endpoints are not visible because the mute participants was initiated by the MCU. Therefore, it is recommended to inform the participants that their audio is muted by using the *Closed Caption* or *Message Overlay* functions.
- When the *Mute Participants Except Lecturer* option is enabled in the *Conference Profile* settings, all conferences to which this profile is assigned will start with this option enabled. All participants, except for the designated lecturer, are muted.
- The *Mute Participants Except Lecturer* option can be enabled at any time after the start of the conference. It allows all the conference participants to converse before the lecturer joins the conference or before they are muted.
- The *Mute Participants Except Lecturer* option can be disabled during an ongoing conference, thereby unmuting all the participants in the conference.
- If the endpoint of the designated lecturer is muted when the lecturer connects to the conference, the lecturer remains muted until the endpoint has been unmuted.
- When you replace a lecturer, the MCU automatically mutes the previous lecturer and unmutes the new lecturer.
- When you disconnect a lecturer from the conference or the lecturer leaves the conference, all participants remain muted but are able to view participants in regular video layout until the you disable the *Mute Participants Except Lecturer* option.
- A participant can override the *Mute Participants Except Lecturer* option by activating the *Mute All Except Me* option using the appropriate DTMF code, provided the participant has authorization for this operation in the IVR Services properties. The lecturer audio is muted and the participant audio is unmuted. You can reactivate the *Mute Participants Except Lecturer* option after a participant has previously activated the *Mute All Except Me* option. The participant is muted and the lecturer, if designated, is unmuted.
- In cascaded conferences, all participants (including the link participants) except the lecturer are muted. Only the lecturer is not muted.

Enabling the Mute Participants Except Lecturer Option

The *Mute Participants Except Lecturer* option is enabled or disabled (default) in the *Conference Profile* or in an ongoing conference in the *Profile Properties - Audio Settings* tab.



When the *Mute Participants Except Lecturer* option is enabled and a conference has started, the **Mute by MCU** icon is displayed in the *Audio* column in the *Participants* pane of each participant that is muted.



Permanent Conference

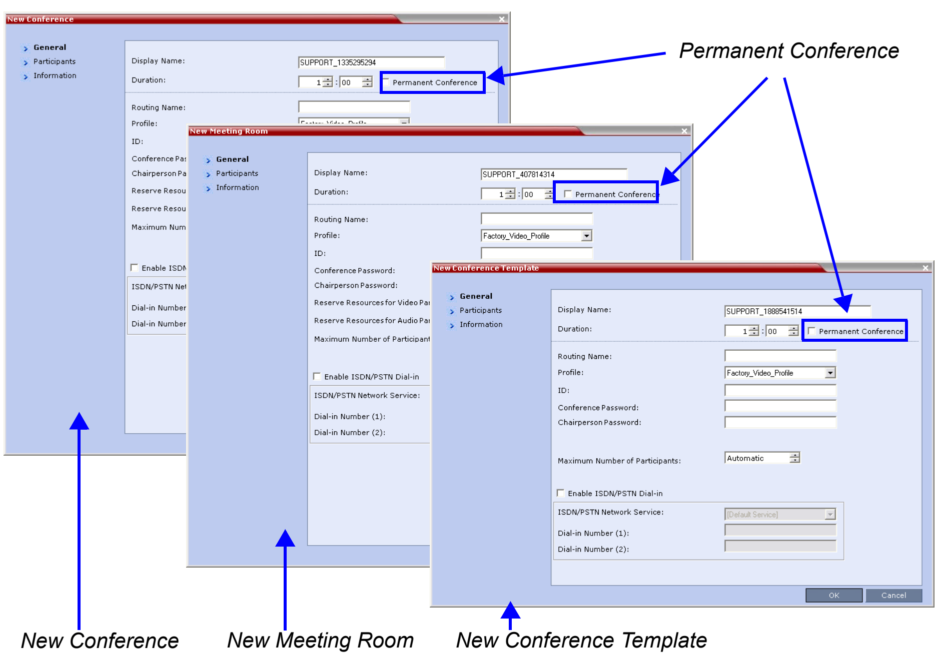
A *Permanent Conference* is an ongoing AVC or SVC conference with no pre-determined *End Time* continuing until it is terminated by an administrator, operator or chairperson.

Guidelines

- Resources are reserved for a *Permanent Conference* only when the conference has become ongoing.
- Resources are allocated to a *Permanent Conference* according to the *Reserve Resources for Video Participants* field. If the number of defined dial-out participants exceeds the value of this field, the RMX automatically replaces the number in the *Reserve Resources for Video Participants* field with the number of defined dial-out participants in the *Permanent Conference.*
- *Auto Terminate* is disabled in *Permanent Conferences*.
- If participants disconnect from the *Permanent Conference*, resources that were reserved for its video and audio participants are released.
- *Entry Queues*, *Conference Reservations* and *SIP Factories* cannot be defined as *Permanent Conferences*.
- Additional participants can connect to the conference, or be added by the operator, if sufficient resources are available.
- The maximum size of the *Call Detail Record* (*CDR*) for a *Permanent Conference* is 1MB.

Enabling a Permanent Conference

The *Permanent Conference* option is selected in the *New Conference, New Meeting Room* or *New Conference Templates* dialog boxes.



Closed Captions (AVC Only)

Endpoints can provide real-time text transcriptions or language translations of the video conference by displaying captions. The captions for a conference may be provided by the captioner who is present in the conference, or the captioner may use a telephone or web browser to listen to the conference audio. When the captioner sends a unit of text, all conference participants see it on the main monitor for 15 seconds. The text then disappears automatically.

The captioner may enter caption text using one of the following methods:

- Remotely, via a dial-up connection to the system's serial RS-232 port.
- In the room using equipment connected directly to the serial port.
- In the room or remotely, using the Polycom HDX web interface.

Closed Captions Guidelines

- The captions display properties are configured on the endpoint sending the captions.
- *Closed Captions* content is defined from the endpoint. The RMX only transmits it to the endpoints.
- When enabled, captions are available to all endpoints supporting FECC.
- Captions are supported in H.323 and SIP connections.
- The FECC indications during ongoing conferences are used when sending captions.
- When *Closed Captions* option is enabled for the MCU, muting an endpoint may cause the display of the "Far Mute" indication on all the screens of the endpoints connected to the conference.
- The *Closed Captions* option is not supported in cascading conferences (captions they can only be viewed in the local conference) as FECC is not supported in cascading links.
- Site name display is not affected by captions display.
- Captions are supported by the RMX in the following configurations and conferencing modes:
  — *MPM, MPM+* and *MPMx Card Configuration Modes*.
  — *AVC* conferencing mode.
  — Encrypted and non-encrypted conferences.
  — Conferences with Content.

From *Version 7.1*, *MPM* media cards are not supported.

Enabling Closed Captions

Captions are enabled by a system flag. By default, *Closed Captions* are disabled.

To change the flag value:

1 On the RMX menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.

2 In the *MCMS_PARAMETERS* tab, click the **New Flag** button.
The *New Flag* dialog box is displayed.

3 In the *New Flag* field enter **ENABLE_CLOSED_CAPTION**.

4 In the *Value* field enter **YES** to enable *Closed Captions* or **NO** to disable their display.

5 Click **OK** to close the *New Flag* dialog box.
The new flag is added to the flags list.

6 Click **OK** to close the *System Flags* dialog box.

For flag changes (including deletion) to take effect, reset the MCU. For more information, see "*Resetting the RMX”* on page **21-69**.

5

Cascading Conferences

> Cascading information applies to AVC Conferencing Mode only. Cascading is not supported with SVC Conferencing Mode.

Cascading enables administrators to connect one conference directly to one or several conferences, depending on the topology, creating one large conference. The conferences can run on the same MCU or different MCUs.

There are many reasons for cascading conferences, the most common are:

- Connecting two conferences on different MCUs at different sites.
- Utilizing the connection abilities of different MCUs, for example, different communication protocols, such as, serial connections and ISDN, etc....

The following cascading topologies are available for cascading:

- **Basic Cascading** - only two conferences are connected (usually running on two different RMXs). The cascaded MCUs reside on the same network.
- **Star Cascading** - one or several conferences are connected to one master conference. Conferences are usually running on separate MCUs. The cascaded MCUs reside on the same network.
- **MIH (Multi-Hierarchy) Cascading** - several conferences are connected to each other in Master-Slave relationship. The cascaded MCUs can reside on different networks.

System configuration and feature availability change according to the selected cascading topology.

Video Layout in Cascading conferences

Cascade links are treated as endpoints in CP conferences and are allocated resources according to "*Default Minimum Threshold Line Rates and Resource Usage Summary*" on page **3-12**. Cascaded links in 1x1 video layout are in SD resolution.

When cascading two conferences, the video layout displayed in the cascaded conference is determined by the selected layout in each of the two conferences. Each of the two conferences will inherit the video layout of the other conference in one of their windows.

In order to avoid cluttering in the cascaded window, it is advised to select appropriate video layouts in each conference before cascading them.

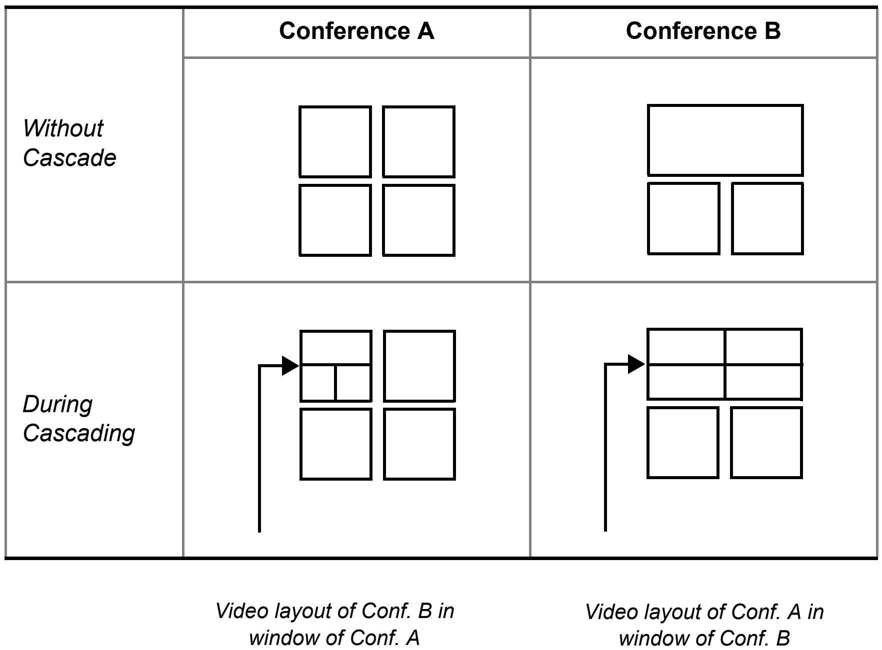


Figure 5-1 *Video Layouts in Cascaded Conferences*

Guidelines

To ensure that conferences can be cascaded and video can be viewed in all conferences the following guidelines are recommended:

- The same version installed on all MCUs participating the cascading topology
- The same license installed on all MCUs participating the cascading topology
- Same Conference Parameters are defined in the Profile of the conferences participating in the cascading topology
  - — Conference line rates should be identical
  - — Content rate should be identical
  - — Same encryption settings
- DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences
- DTMF forwarding is suppressed
- The video layout of the link is set to 1x1 by the appropriate system flag.
- When the Mute Participants Except Lecturer option is enabled in the Conference Profile, all participants (including the link participants) except the lecturer are muted. Only the lecturer is not muted.

Flags controlling Cascade Layouts

- Setting the **FORCE_1X1_LAYOUT_ON_CASCADED_LINK _CONNECTION** *System Flag* to **YES** (default) automatically forces the cascading link to

Full Screen (1x1) in CP conferences, hence displaying the speaker of one conference to a full window in the video layout of the other conference.

Set this flag to **NO** when cascading between an RMX and an MGC that is functioning as a Gateway, if the participant layouts on the MGC are not to be forced to 1X1.

- Setting the **AVOID_VIDEO_LOOP_BACK_IN_CASCADE** *System Flag* to **YES** (default) prevents the speaker's image from being sent back through the participant link from the cascaded conference. This can occur in cascaded conferences with conference layouts other than 1x1. It results in the speaker's own video image being displayed in the speaker's video layout.

  Guidelines

  This option is supported with:

  — With *MPM+* and *MPMx* cards.

  — In *H.323, SIP* and *ISDN* environments.

  — For *Basic Cascading* of *Continuous Presence,* and *Video Switched* conferences. If a *Master MCU* has two slave MCUs, participants connected to the slave MCUs will not receive video from each other.

  — Video resolution will be according to the *Resolution Configuration*, or *VSW* profile.

For more details on defining system flags, see "*Modifying System Flags"* on page **22-1**.

DTMF Forwarding

When two conferences are connected over an IP link, DTMF codes from one conference are not forwarded to the second conference with the exception of the following operations that are available throughout the conference and the forwarding of their DTMF codes is not suppressed (i.e. they will apply to both conferences):

- Terminate conference.
- Mute all but me.
- Unmute all but me.
- Secure conference.
- Unsecure conference.

> During cascading between a gateway and a conference **all** DTMF codes are forwarded from the gateway to the conference and vice versa.

Play Tone Upon Cascading Link Connection

The RMX can be configured to play a tone when a cascading link between conferences is established. The tone is played in both conferences.

This tone is not played when the cascading link disconnects from the conferences.

The tone used to notify that the cascading link connection has been established cannot be customized.

The option to play a tone when the cascading link is established is enabled by setting the *System Flag*: **CASCADE_LINK_PLAY_TONE_ON_CONNECTION** to **YES**.

Default value: **NO**.

The tone volume is controlled by the same flag as the IVR messages and tones: **IVR_MESSAGE_VOLUME**.

Basic Cascading

In this topology, a link is created between two conferences, usually running on two different MCUs. The MCUs are usually installed at different locations (states/countries) to save long distance charges by connecting each participant to their local MCU, while only the link between the two conferences is billed as long distance call.

- This is the only topology that enables both IP and ISDN cascading links:
  - — When linking two conferences using an IP connection, the destination MCU can be indicated by:
    - IP address
    - H.323 Alias
  - — If IP cascading link is used to connect the two conferences, both MCUs must be located in the same network.
- One MCU can be used as a gateway.
- The configuration can include two RMXs or one RMX and one MGC.
- *Multiple Cascade Links* enabling *Cascading* between RMXs hosting conferences that include *Immersive Telepresence Rooms (ITP)* such as *Polycom's OTX* and *RPX Room Systems* can be defined. For more information see "*Multiple Cascade Links"* on page **4-62**.

Basic Cascading using IP Cascaded Link

In this topology, both MCUs can be registered with the same gatekeeper or the IP addresses of both MCUs can be used for the cascading link. Content can be sent across the Cascading Link.

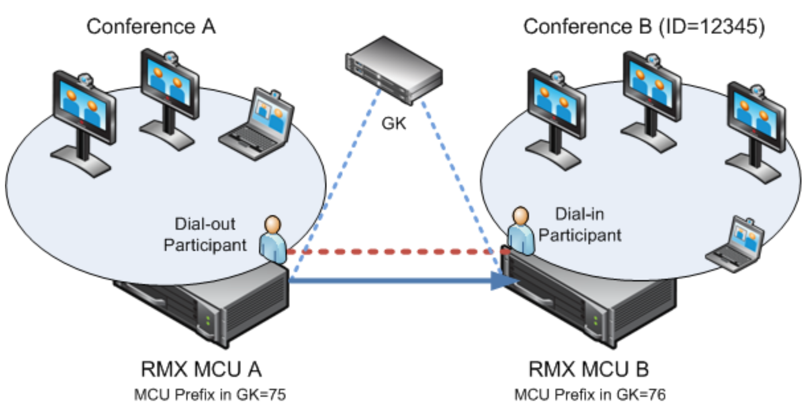


Figure 5-2 *Basic Cascading Topology - IP Cascading Link*

For example, MCU B is registered with the gatekeeper using 76 as the MCU prefix.

The connection between the two conferences is created when a dial out IP participant is defined (added) to conference A whose dial out number is the dial-in number of the conference or Entry Queue running on MCU B.

Dialing Directly to a Conference

Dial out IP participant in conference A dials out to the conference running on MCU B entering the number in the format:
[MCU B Prefix/IP address][conference B ID].

For example, if MCU B prefix is 76 and the conference ID is 12345, the dial number is **7612345**.

Dialing to an Entry Queue

When dialing to an Entry Queue, the dial out participant dials the MCU B prefix or IP address of MCU B and the Entry Queue ID in the format:

[MCU B Prefix/IP address][EQ B ID].

For example, if MCU B prefix is 76 and the Entry Queue ID is 22558, the dial number is **7622558**.

When the participant from conference A connects to the Entry Queue, the system plays to all the participants in Conference A the IVR message requesting the participant to enter the destination conference ID.

At this point, the Conference A organizer or any other participant in the conference can enter the required information for the IVR session using DTMF codes. For example, the meeting organizer enters the destination conference ID - **12345**.

Any DTMF input from conference A is forwarded to the Entry Queue on MCU B to complete the IVR session and enable the move of the participant to the destination conference B.

Once the DTMF codes are entered and forwarded to the Entry Queue on MCU B, the IVR session is completed, the participant moved to the destination conference and the connection between the two conferences is established.

Automatic Identification of the Cascading Link

In both dialing methods, the system automatically identifies that the dial in participant is an MCU and creates a Cascading Link and displays the link icon for the participant (). The master-slave relationship is randomly defined by the MCUs during the negotiation process of the connection phase.

Basic Cascading using ISDN Cascaded Link

ISDN connection can be used to link between two MCUs or MCU and gateway and create a cascading conference. Content can be sent across the ISDN Cascading Link.

Network Topologies Enabling H.239 Content Over ISDN Cascaded Links

ISDN Cascaded links that support H.239 Content can be created between two gateways, gateway-to-MCU or between two MCUs in the following network topologies:

- **Gateway to Gateway**

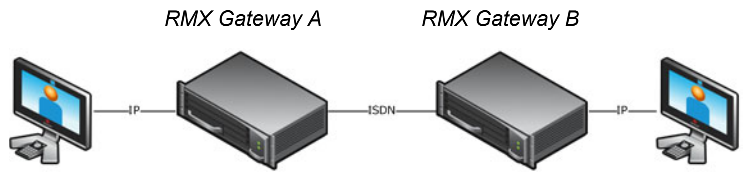


Figure 5-3 *Gateway to Gateway Topology*

In this topology, an IP participant calls another IP participant over an ISDN link between two gateways.

- **Gateway to MCU**

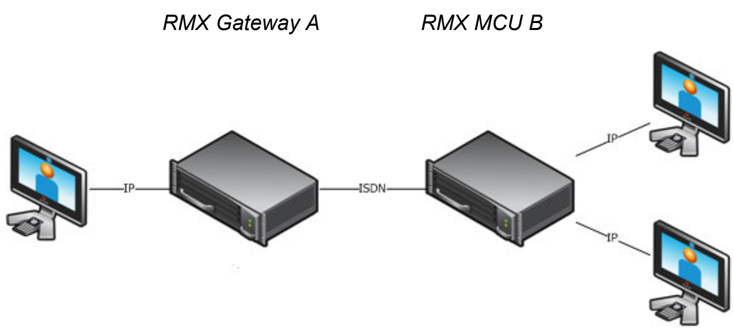


Figure 5-4 *Gateway to MCU/ MCU to Gateway Topology*

In this topology, an IP participant calls a conference running on an MCU via a gateway and over an ISDN link.

- **MCU to MCU**

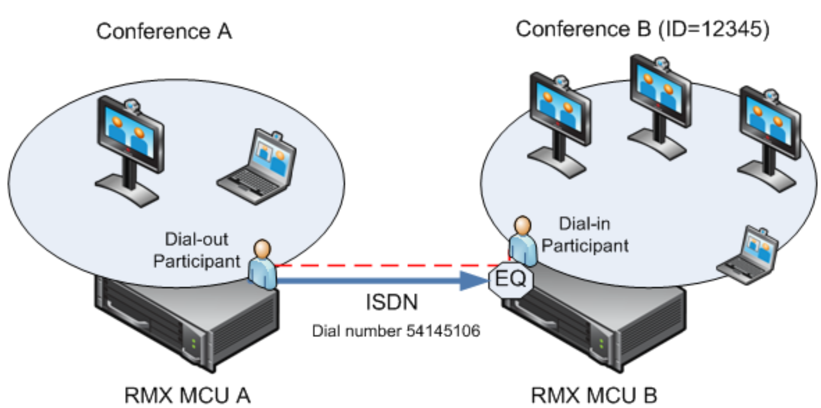


Figure 5-5 *Cascading Between Two MCUs Using an ISDN Link*

In this topology, an ISDN participant from conference running on MCU A calls a conference running on MCU B over an ISDN link.

Guidelines

- Content is restricted. When another endpoint wants to send content, the first endpoint must stop sending content before the second endpoint can initiate or send content.
- Endpoints that do not support H.239 can receive the Content using the *Send Content to Legacy Endpoints* option.

- When a participant joins a conference with active Content, content cannot be viewed by the new participant. Restart the Content.
- Cascaded MCUs/Gateways must be registered with the same Gatekeeper or neighboring Gatekeepers. MCUs and endpoints must also be registered with Gatekeepers.
- Gateway/MCU calls require definition of IVR Services. For more information see "*Defining the IVR Service for Gateway Calls*" on page **19-14**.

> In version 7.1, H.239 content protocol is H.263 when sent over ISDN or H.323 Cascading link.

Gateway to Gateway Calls via ISDN Cascading Link

When H.323 participants connects to another IP participants via a *Gateway to Gateway* call over an ISDN link, the dialing string includes the following components:

[GW A prefix in GK] - the prefix with which the RMX (gateway) is registered to the gatekeeper.

[GW Profile ID] - The ID of the Gateway Profile defined on Gateway A to be used for routing the call to the Gateway B.

[GW Profile ISDN/PSTN number] - the dial-in number assigned to the Gateway Profile defined on Gateway B, including the required country and area codes.

Information required that is not part of the dialing string:

[Destination number] - the destination number as alias, IPv4 address or ISDN/PSTN number of participant B.

The dialing string format:

H.323 Participants connecting to another IP participant via a *Gateway to Gateway* call over an ISDN link enter a dial string using the format:

```
<GW A Prefix in GK><Gateway Profile_ID on GW A>*<Destination ISDN
Dial-in number assigned to the Gateway Session Profile GW
B>*<Destination Number, participant>
```

For example:

GW A prefix in Gatekeeper - (not used with SIP)	22
Gateway Profile ID in GW A	9999
ISDN Dial-in Number assigned to the Gateway Session Profile GW B	4444103
IP Participant Alias	3456

H.323 participant dials: 229999*4444103 and when prompted for the Destination number enters 3456 followed by the pound key (#) using DTMF codes.

SIP Participants connecting to another IP participant via a *Gateway to Gateway* call over an ISDN link enter a dial string using the format:

```
<Gateway Profile_ID on GW A>@<Central Signaling IP GW
A>*<Destination ISDN Dial-in number assigned to the Gateway Session
Profile GW B>*<Destination Number, participant>
```

For example:

If Central Signaling IP address of Gateway A is 172.22.177.89, SIP participant dials: 9999@ 172.22.177.89* 4444103 and when prompted for the Destination number enters 3456 followed by the pound key (#) using DTMF codes.

Gateway to MCU Calls via ISDN Cascading Link

When H.323 participants connects to a conference/Meeting Room via a *Gateway to MCU* call over an ISDN link, the dialing string includes the following components:

The dialing string includes the following components:

`[GW A prefix in GK]` - the prefix with which Gateway A is registered to the gatekeeper.

`[GW Profile ID on GW A]` - The ID of the Gateway Profile on GW A to be used for routing the call to the Meeting Room/conference running on MCU B.

`[Conference/Meeting Room/Entry Queue ISDN/PSTN number]` - the dial-in number assigned to the Entry Queue/Meeting Room/Conference defined on MCU B, including the required country and area codes.

Information required that is not part of the dialing string:

[`Destination Conference ID`] - Only if using the Entry Queue on MCU B for routing calls or creating new ad hoc conferences. The ID of the destination conference on MCU B.

The dialing string format:

```
<GW A Prefix in GK><Gateway Profile_ID on GW A>*<ISDN Number
assigned to the Meeting Room/Conference/Entry Queue>
```

For Example:

GW A prefix in Gatekeeper - (not used with SIP)	22
Gateway Profile ID in GW A	9999
ISDN Dial-in Number assigned to the Entry Queue/MR/conference	4444100

H.323 participant dials: 229999*4444100.

SIP participant dials (if Central Signaling IP address of Gateway A is 172.22.177.89): 9999@ 172.22.177.89 IP* 4444100.

If dialing an Entry Queue, when prompted for the Destination number enters 3456 followed by the pound key (#) using DTMF codes to create a new conference or join an ongoing conference with that ID.

MCU to MCU Calls via ISDN Cascading Link

A dial out ISDN participant is defined (added) to conference A running on MCU A. The participant's dial out number is the dial-in number of the Entry Queue or conference running on MCU B (for example 54145106).

MCU A dials out to an Entry Queue or conference B running on MCU B using the Entry Queue number (for example 54145106) or the conference number.

When the participant, who is a dial-in participant in conference B, connects to the Entry Queue, the system plays to all the participants in Conference A the IVR message requesting the participant to enter the destination conference ID (or if connecting to a conference directly, the participant is requested to enter the conference password).

At this point the Conference A organizer or any other participant in the conference can enter the required information for the IVR session using DTMF codes. For example, the meeting organizer enters the destination conference ID - 12345.

Any DTMF input from conference A is forwarded to the Entry Queue on MCU B to complete the IVR session and enable the move of the participant to the destination conference B.

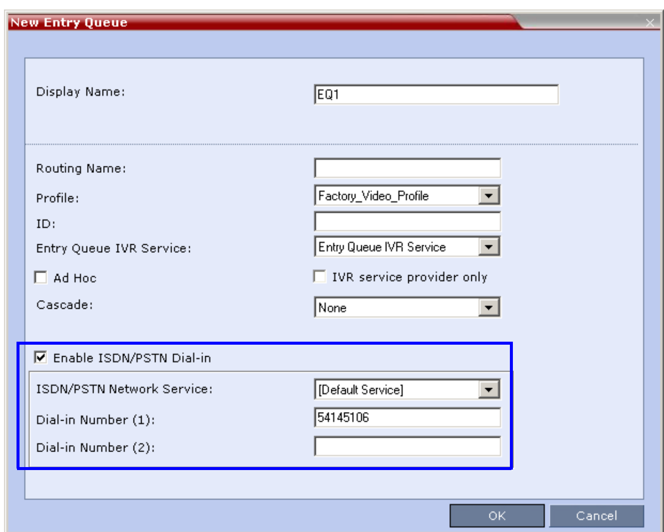
Once the DTMF codes are entered and the IVR session is completed, the participant is connected to the conference and the connection between the conferences is established. The system automatically identifies the calling participant as an MCU and the connection is identified as a cascading link and the cascading link icon is displayed for the participant

().

RMX Configuration Enabling ISDN Cascading Links

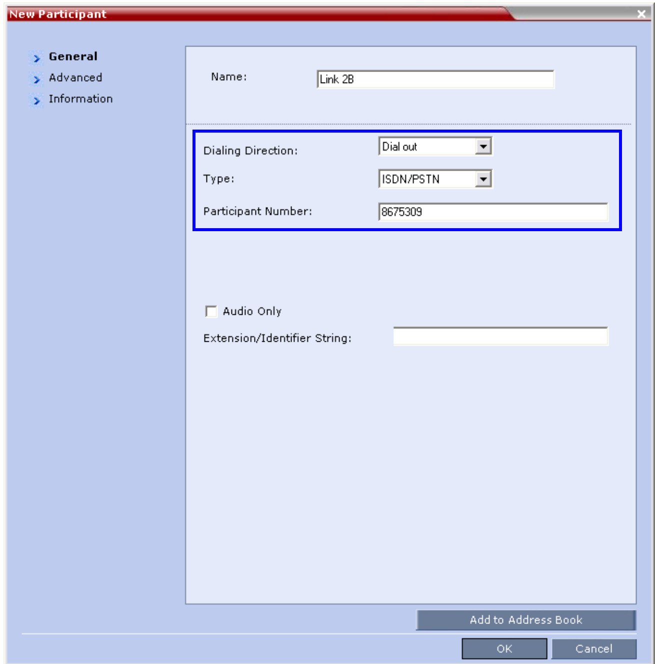
To enable Gateway-to-Gateway, Gateway-to-MCU and MCU-to-MCU calls over ISDN Cascading links, the following configurations are required:

- Modifying the IP Network Service to include the MCU Prefix in the Gatekeeper (in the Gatekeepers dialog box). For more details, see "*Modifying the Default IP Network Service"* on page **16-11**.
- ISDN Network Service is configured in both MCUs. For more details, "*Modifying an ISDN/PSTN Network Service"* on page **16-47**.
- Configuring a Gateway Profile and assigning dial-in ISDN/PSTN numbers. For details, see "*Defining the Gateway Profile"* on page **19-18**.
- Configure the *Entry Queue* or conference (for direct dial-in) is enabled for ISDN connection and a dial-in number is assigned (for example 54145106).



- Defining the dial-in ISDN participant in MCU B and Dial-out ISDN participant in MCU A (for MCU-to-MCU cascading conferences).

A dial out ISDN participant is defined (added) to conference A. The participant's dial out number is the dial-in number of the Entry Queue or conference running on MCU B (for example 54145106).



MCU A dials out to an Entry Queue or conference B running on MCU B using the Entry Queue number (for example 54145106) or the conference number.

Conference Profile Definition

The following table lists the recommended Meeting Room/Conference Profile parameters setting when routing ISDN cascaded calls.

Table 5-1 Recommended Conference Profile Options Setting

Line Rate	Motion	Sharpness	Encryption	LPR
128	√			
128		√		
128	√			√
128	√		√	√
256	√			
256		√		
256	√			√
256	√		√	√
384	√			
384		√		
384	√			√

Table 5-1 Recommended Conference Profile Options Setting (Continued)

Line Rate	Motion	Sharpness	Encryption	LPR
384	√		√	√
512	√			
512		√		
512	√			√
512	√		√	√
768	√			
768		√		
768	√			√
768	√		√	√

Since the remote participant settings are unknown, it is recommended that the gateway or endpoint be configured to support a higher line rate (for example, 768 Kbps) to allow flexibility during endpoint capability negotiations.

MCU Interoperability Table

The following table lists the different MCU and Gateway configurations that are supported or implemented when routing Cascaded ISDN calls.

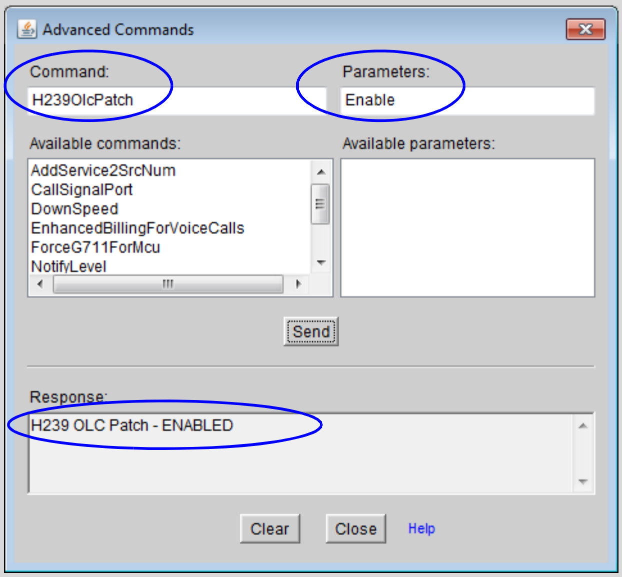
Table 5-2 MCU Interoperability Table

		Scenario	Version(s)
RMX Gateway	RMX MCU	User calls via a Gateway to a Remote Conference (user to conference)	RMX v. 7.1
RMX Gateway	RMX Gateway	User calls via a Gateway to a Remote User behind Gateway (user to user)	RMX v. 7.1
RMX MCU	RMX MCU	A dial out participants calls to a remote conference (conference to conference)	RMX v. 7.1
RMX MCU	RMX Gateway	A dial out participants calls to a remote User behind a Gateway (Conference to User)	RMX v. 7.1
Endpoint	RMX Gateway	User calls directly to a remote user behind a Gateway (User to User)	RMX v. 7.1
RMX MCU	Codian Gateway	Dial out participants use a fixed rule behind the Codian Gateway.	RMX v. 7.1 Latest Codian version
RMX Gateway	Codian Gateway	Dial out participants use a fixed rule behind the Codian Gateway.	RMX v. 7.1 Latest Codian version
Codian Gateway	RMX MCU	User calls via a Codian Gateway to a Remote Conference (user to conference)	RMX v. 7.1 Latest Codian version

Table 5-2 MCU Interoperability Table (Continued)

		Scenario	Version(s)
Codian Gateway	RMX Gateway	User calls via a Codian Gateway to a Remote User behind RMX Gateway (user to user)	RMX v. 7.1 Latest Codian version
RMX MCU	Radvision Gateway	User calls via a Radvision Gateway to a Remote User behind RMX Gateway (user to user)	RMX v. 7.1 Latest Radvision version
RMX Gateway	Radvision Gateway	User calls via a Radvision Gateway to a Remote User behind RMX Gateway (user to user)	RMX v. 7.1 Latest Radvision version
Radvision Gateway	RMX MCU	User calls via a Radvision Gateway to a Remote Conference (user to conference)	RMX v. 7.1 Latest Radvision version
Radvision Gateway	RMX Gateway	User calls via a Radvision Gateway to a Remote User behind RMX Gateway (user to user)	RMX v. 7.1 Latest Radvision version
Endpoint	RMX Gateway	User calls directly to a DMA controlled environment	RMX v. 7.1
RMX MCU	RMX Gateway	A dial out participants calls to a remote conference on a DMA controlled environment	RMX v. 7.1

- On the Codian gateway Content is not supported with line rates of 128Kbps and below.
- When using the following topology:
  H.323 endpoint ->Codian Gateway -> ISDN Link -> RMX -> H.323 endpoint, the Codian Gateway is unable to send DTMF and the call is disconnected (VNGFE- 3587).
- Sending Content from a participant over Radvision Gateway to a conference/participant, the GWP20 patch must be installed in the RadVision gateway:
  On the Radvision gateway, open the GWP20 User Interface. Click *Settings/Advanced Commands*. In the *Command* box enter **H239OlcPatch.** In the **Parameters** box enter **Enable** and then click **Send**.



Suppression of DTMF Forwarding

Forwarding of the DTMF codes from one conference to another over an ISDN cascading link is not automatically suppressed as with IP cascading link and it can be limited to basic operations while suppressing all other operations by a system flag: DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS.

System Flag Settings

The **DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS** flag determines the time period (in seconds) that MCU A will forward DTMF inputs from conference A participants to MCU B.

Once the timer expires, most of the DTMF codes (excluding five operations as for IP links) entered in conference A will not be forwarded to conference B. This is done to prevent an operation requested by a participant individually (for example, mute my line) to be applied to all the participants in conference B.

Flag range (in seconds): **0 - 360000**

This flag is defined on MCU A (the calling MCU).

If a flag is not listed in the *System Flags* list it must be added to the *system.cfg* file before it can be modified. For more details on defining system flags, see "*Modifying System Flags"* on page **22-1**.

Star Cascading Topology

In the Star topology (as well as in the Basic topology), the MCUs are usually installed at different locations (states/countries) and participants connect to their local MCU to facilitate the connection and save long distance call costs. Star Topology Cascading requires that all cascaded MCUs reside on the same network.

Although participants in Star Cascading conferences can connect to their local conference using H.323, SIP and ISDN, the Cascading Links between conferences must connect via H.323.

Content sharing is available to all conferences over the H.323 Cascading Link.

In this topology, the MCUs are networked together using two modes:

- Master-Slave Cascading
- Cascading via Entry Queue

Master-Slave Cascading

It is similar to MIH (Multi Hierarchy) cascading, with only two levels: one *Master MCU* on level 1 and several *Slave* MCUs on level 2.

The cascading hierarchy topology can extend to four levels (Figure 5-9) and should be deployed according to the following guidelines:

- If an RMX is deployed on level 1:
  - — RMX systems can be used on level 2
  - — MGC with version 9.0.4 can be used on level 2 if RMX version 7.0.2 and higher is deployed in level 1
- If an *MGC* is deployed on level 1:
  - — MGC or RMX can be used on level 2.

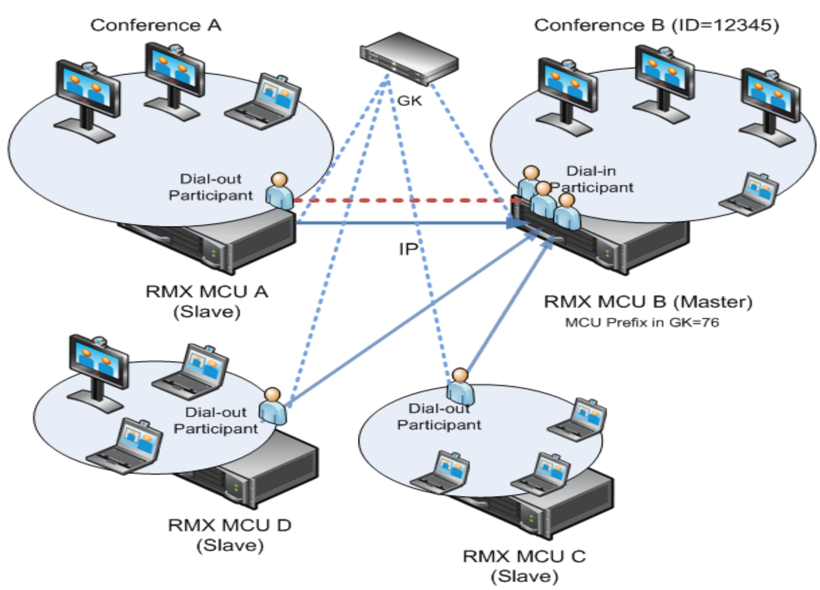


Figure 5-6 *Master-Slave Star Cascading Topology*

- When creating a cascading link between two RMXs:
  - — The RMXs operate in CP (Continuous Presence) mode.
- When creating a cascading link between MGCs and RMXs:
  - — The MGCs can only operate in VSW mode.

The following table summarizes *Video Session Modes* line rate options that need to be selected for each conference in the cascading hierarchy according to the cascading topology:

Table 6 *MIH Cascading – Video Session Mode and Line Rate*

Topology	MCU Type	Video Session Mode	Line Rate	Endpoint
Level 1	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s	HDX
Level 2	RMX			
Level 1	RMX	CP - CIF	768Kb/s, 2Mb/s	VSX
Level 2	RMX			
Level 1	MGC	CP - CIF 263	768Kb/s, 2Mb/s	HDX, VSX
Level 2	RMX	CP - CIF 264		
Level 1	MGC	VSW - HD	1.5Mb/s	HDX
Level 2	RMX	VSW HD		

To establish the links between two RMXs requires the following procedures be performed:

- Establish the Master-Slave relationships between the cascaded conferences by defining the dialing direction.
- Create the Master and Slave conferences, defining the appropriate line rate.
- Create a cascade-enabled *Dial-out Participant* link in the Master conference
- Create a cascade-enabled *Dial-in Participant* link in the Slave conference.

Creating a Cascade Enabled Dial-out/Dial-in Participant Link

The connection between two cascaded conferences is established by a cascade enabled dial-out and dial-in participants, acting as a cascades link.

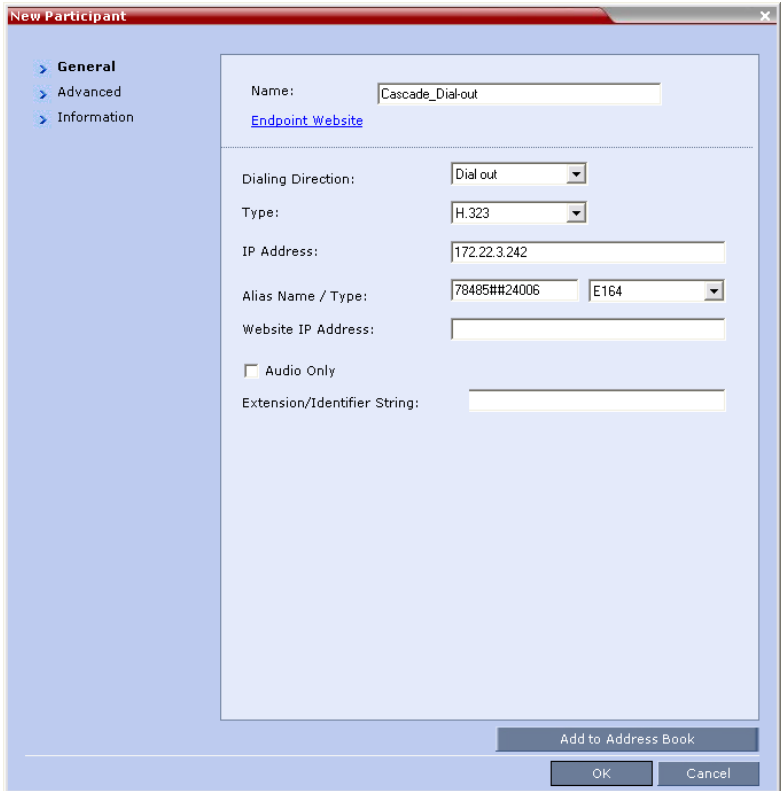
The dialing direction determines whether the dial-out participant is defined in the conference running on the Master MCU or the Slave MCU. For example, if the dialing direction is from the Master conference on level 1 to the Slave conference on level 2, the dial-out participant is defined in the Master conference on level 1 and a dial-in participant is defined in the Slave conference running on the MCU on level 2.

If the cascade-enabled dial-out participant always connects to the same destination conference on the other (second) MCU, the participant properties can be saved in the Address Book of the MCU for future repeated use of the cascaded link.

To define the dial-out cascade participant link:

1. In the *Conferences* pane, select the conference.
2. In the *Participants* pane, click **New Participant** ( ).

The *New Participant - General* dialog box is displayed.



3 Define the following parameters:

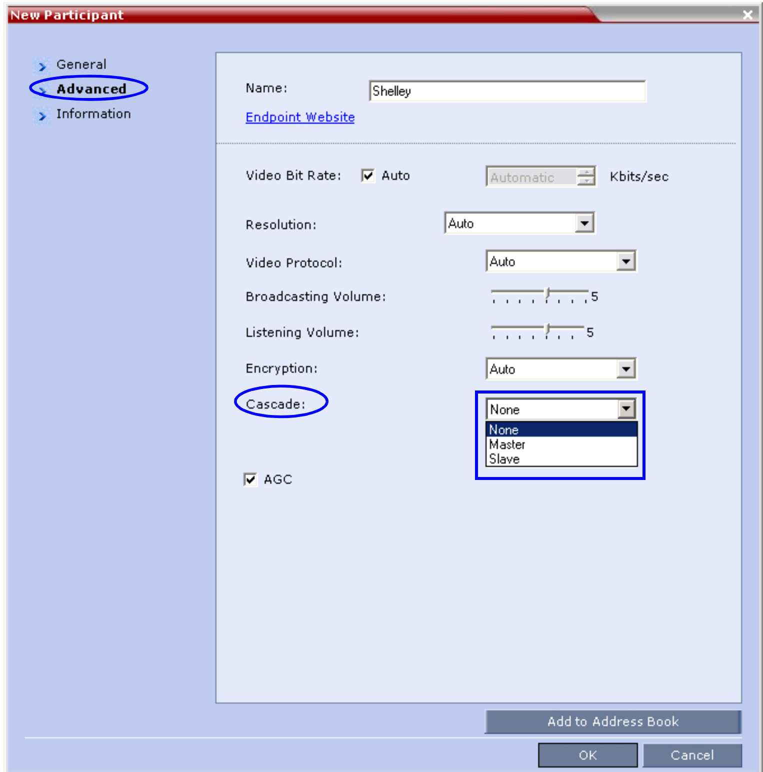
Table 7 New Participant – Dial-out Cascade Link

Field	Description
Display Name	Enter the participant name
Dialing Direction	Select **Dial-out**.
Type	Select **H.323**.
IP Address	Enter the IP address of the Signaling Host of the MCU running the other (second) conference, where the cascade enabled Entry Queue is defined.

Table 7 *New Participant – Dial-out Cascade Link (Continued)*

Field	Description
Alias Name	If you are using the target MCU IP address, enter the Conference ID of the target conference. For example: `24006` If a gatekeeper is used, instead of the IP address, you can enter the prefix of the target MCU as registered with the gatekeeper, as part of the dialing string and the conference ID in the format: **`<Target MCU Prefix>`**`<Conference_ID>` For example: **`925`**`24006` If the conference has a password and you want to include the password in the dial string, append the password to in the dial string after the Conference ID. For example: `92524006`**`##1234`** If the conference has a password and you do not want to include the password in the dial string, set the `ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD` flag to **YES**. For more information see *"Modifying System Flags"* on page **22-1**.
Alias Type	Select **E.164** (digits 0-9, *, #).

4 Click the *Advanced* tab.



5 In the *Cascade* field, select:

— **Slave**, if the participant is defined in a conference running on a Slave MCU.

— **Master**, if the participant is defined in a conference running on the Master MCU.

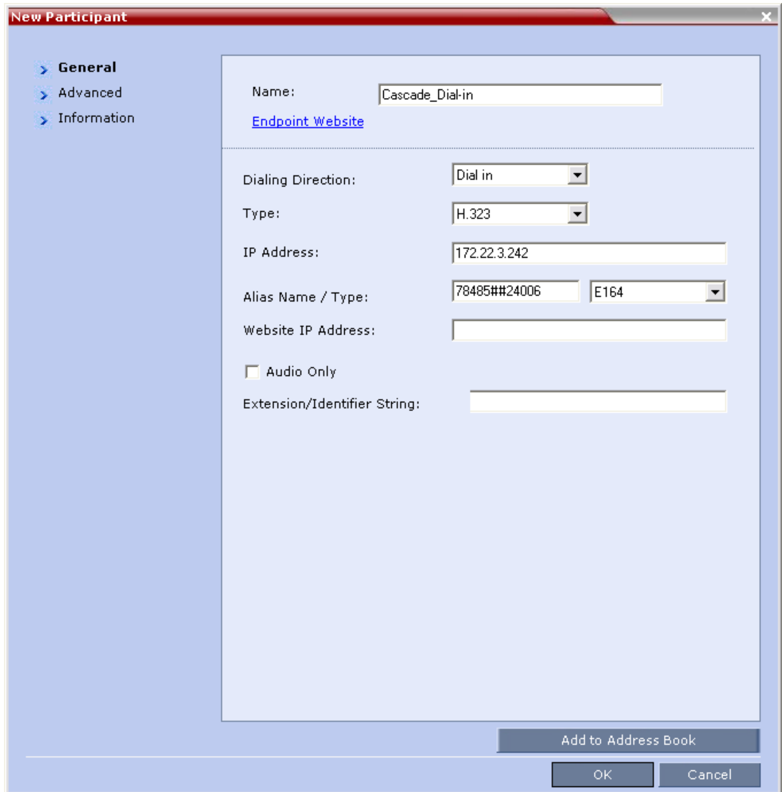
6 Click **OK**.

To define a Dial-in Participant as the cascade link:

This participant is added to the ongoing conference on the *Slave* MCU.

1 In the *Participants* list, click the **New Participant** button( ).

The *New Participant - General* dialog box opens.



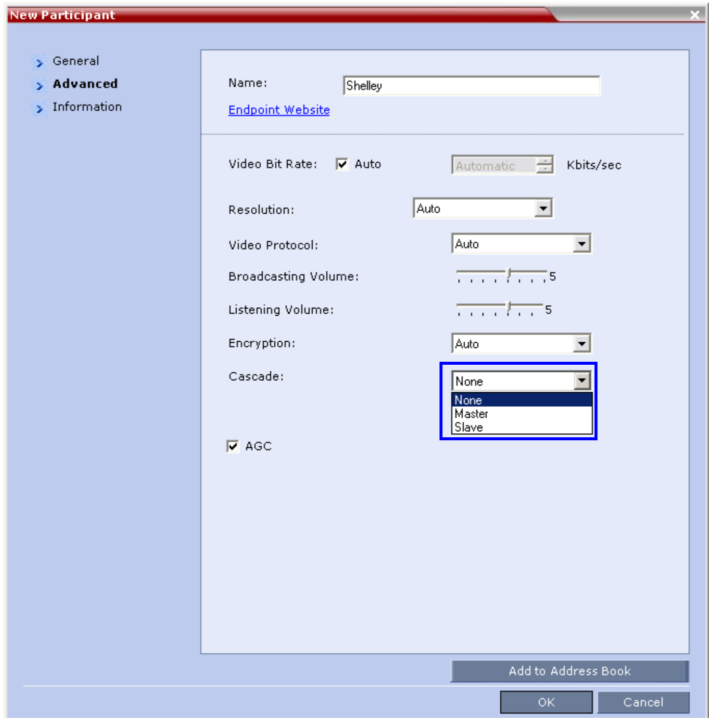
2 Define the following parameters:

Table 5-1 *New Participant – Dial-out Cascade Link*

Field	Description
Display Name	Enter the participant name
Dialing Direction	Select **Dial-in**.
Type	Select **H.323**.
IP Address	**If a gatekeeper is used:** This field is left empty. **If a gatekeeper is not used:** Enter the IP address of the Signaling Host of the MCU running the other conference.
Alias Name	**If a gatekeeper is used:** Enter the **Alias** of the MCU running the other (second) conference. **If a gatekeeper is not used:** This field is left empty.
Alias Type	Select **E.164** (digits 0-9, *, #).

3 Click the **Advanced** tab.

The *Advanced* tab opens.



4 In the *Cascaded Link* field, select:

— **Slave**, if the participant is defined in a conference running on a Slave MCU.

— **Master**, if the participant is defined in a conference running on the Master MCU.

5 Click the **OK** button.

Cascading via Entry Queue

The link between the two conferences is created when a participant that is defined as a dial-out cascaded link in one conference (Conference A) connects to the second conference (Conference B) via a special cascaded Entry Queue (EQ). When MCU A dials out to the cascaded link to connect it to conference A, it actually dials out to the cascaded Entry Queue defined on MCU B.

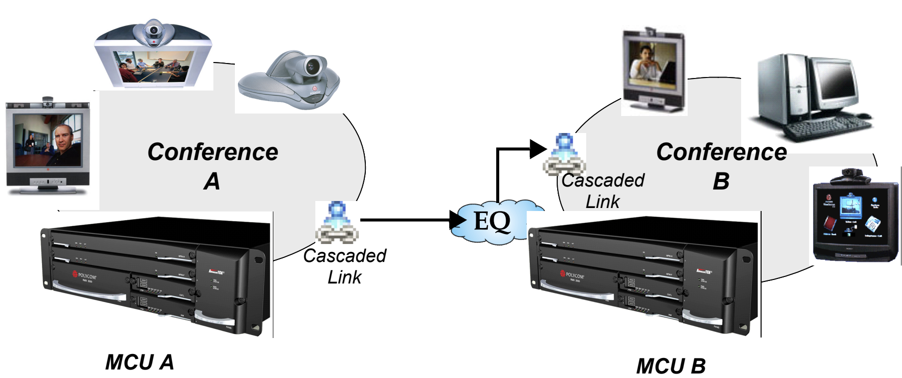


Figure 5-7 Cascaded Conferences - Star Topology

Though the process of cascading conferences mentioned in this section refers to conferences running on two different RMX units, it is possible to cascade conferences running between RMX units and other MCUs.

The following features are not supported by the cascaded link and therefore are not supported in the combined conference:

- **DTMF** codes are enabled in cascaded conference, but only in their local conference. The operations executed via DTMF codes are not forwarded between linked conferences.
- **FECC** (Far End Camera Control will only apply to conferences running in their local MCU).

Enabling Cascading

Cascading two conferences requires that the following procedures are implemented:

- Creating the cascade-enabled Entry Queue

  A cascade-enabled Entry Queue must be created in the MCU hosting the destination conference (Conference B). The cascade-enabled Entry Queue is used to establish the dial-in link between the destination conference and the linked conference and bypassing standard Entry Queue, IVR prompt and video slide display.
- **Creating a cascade-enabled Dial-out link**

  The creation of a cascade-enabled dial-out link (participant) in the linked conference (Conference A). This dial-out participant functions as the link between the two conferences.
- (Optional) Enabling the cascaded linked participant to connect to the linked conference (Conference A) without entering the conference password. This can be done by modifying the default settings of the relevant system flag.

Creating the Cascade-enabled Entry Queue

The cascade-enabled Entry Queue maintains the correct behavior of the cascaded link when it dials into it.

> The cascade-enabled Entry Queue should be used only to connect cascaded links and should not be used to connect standard participants to conferences.

When cascading High Definition (HD) conferences, the cascade-enabled Entry Queue must have the same settings as both cascaded conferences and the participants in both conferences must use the same line rate and HD capabilities as set for the conferences and Entry Queue.

To Define a Cascade-Enabled Entry Queue:

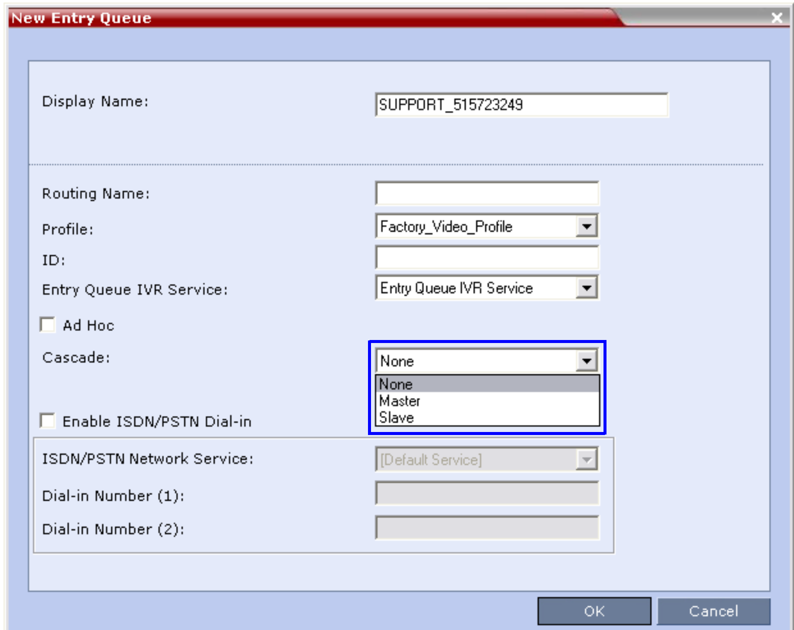
1. In the *RMX Management* pane, click the **Entry Queues** button.

   The *Entry Queues* list pane is displayed.
2. Click the **New Entry Queue**  button.

   The *New Entry Queue* dialog box is displayed.
3. Define the standard Entry Queue parameters (as described in Chapter 3).
4. In the *Cascade* field, select **Master** or **Slave** depending on the Master/Slave relationship.

   — Set this field to **Master** if the Entry Queue is defined on the MCU that is at the center of the topology and other conferences dial into it (acting as the Master).

— Set this field to **Slave** if the Entry Queue is defined on the MCU acting as a Slave, that is, to which the link from the Master MCU (MCU at the center of the topology) is dialing.



If you are defining an HD cascaded Entry Queue, it is recommended to select the same Profile that is selected for both conferences.

5 Click **OK**.

The new Entry Queue enabling cascading is created.

Creating the Dial-out Cascaded Link

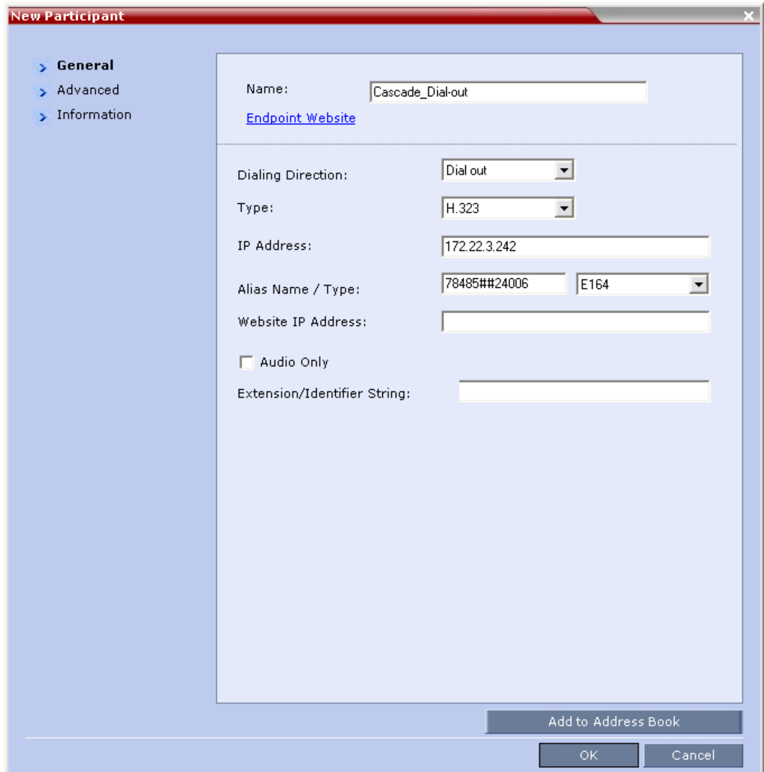
The dial-out link (participant) is created or added in the linked conference (Conference A). The dial-out string defined for the participant is the dialing string required to connect to the destination conference (Conference B) Entry Queue defined on the MCU hosting the destination cascaded conference. The dial-out participant can be defined in the Address Book and added to the conference whenever using the same cascade-enabled Entry Queue and a destination conference (with the same ID and Password).

To define the Dial-out Cascaded Link:

1 Display the list of participants in the linked conference (Conference A).

2 In the *Participant List* pane, click the **New Participant** button.

The *New Participant - General* dialog box is displayed.



3 In the *Name* field, enter a participant name.

4 In the *Dialing Direction* field, select **Dial-out**.

5 In the *Type* list field, verify that **H.323** is selected.

6 There are two methods to define the dialing string:

A Using the MCU's IP Address and the Alias string.

B Using only the Alias string (requires a gatekeeper).

<u>Method A (If no gatekeeper is used):</u>

In the *IP Address* field, enter the IP address of the **Signaling Host** of the MCU hosting the <u>destination</u> conference (in the example, MCU B).

In the *Alias Name/Type* field, enter the ID of the cascade-enabled Entry Queue (EQ), the Conference ID and Password of the destination conference (MCU B) as follows:
EQ ID#Destination Conference ID#Password (Password is optional).

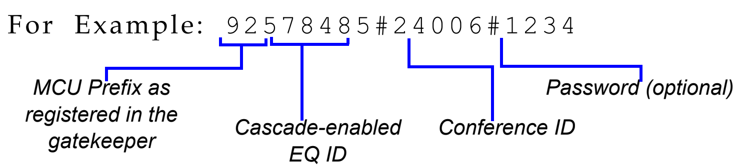
For Example: 78485#24006#1234

Cascade-enabled EQ ID *Destination Conference ID* *Password (optional)*

<u>Method B (Using a gatekeeper):</u>

In the *Alias Name* field, enter the Prefix of MCU B, EQ ID, Destination Conference ID, and Password, as follows:

MCU Prefix EQ ID#Conference ID#Password (Password is optional)

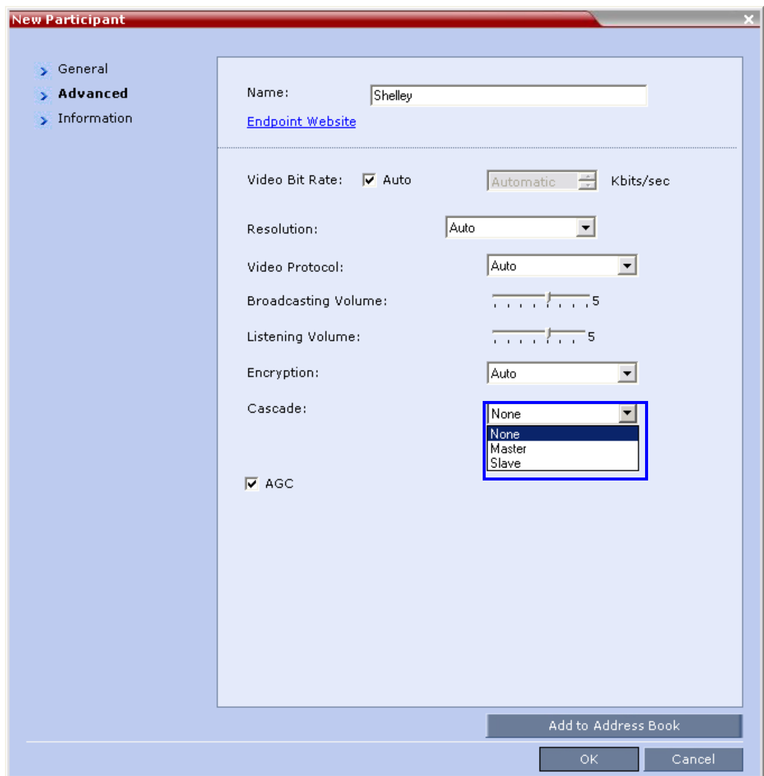


7 Click the **Advanced** tab.

8 In the *Cascade* field, select:

— **Slave**, if the participant is defined in a conference running on a Slave MCU and will connect to the Master MCU (in the center of the topology).

— **Master**, if the participant is defined in a conference running on the Master MCU (in the center of the topology) dialing from the Master MCU to the Slave MCU.



9 Click **OK**.
The cascade-enabled dial-out link is created and the system automatically dials out to connect the participant to the linked conference, as well as the destination conference.

Enabling Cascaded Conferences without Password

If a password is assigned to the linked conference, cascaded links will be prompted for a password when connecting to it (Conference A). Administrators have the option of altering the MCU settings to enable cascaded links to connect without a password.

To enable cascaded links to connect without a password:

1 In the RMX web client connected to MCU A (where the linked conference is running), click **Setup>System Configuration**.
The *System Flags* dialog box opens.

2 Set the **ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD** flag to **YES**.

3 Click **OK**.

For more information, see "*Modifying System Flags"* on page **22-1**.

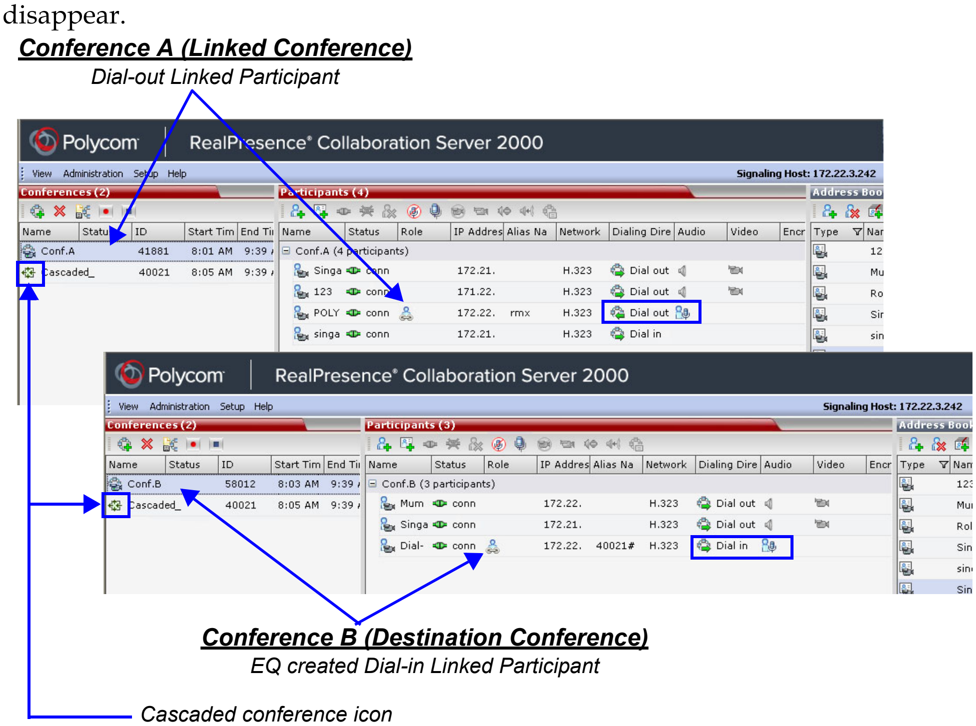
\>> Reset the MCU for flag changes to take effect.

Monitoring Star Cascaded Conferences

To monitor both conferences at the same time, two instances of the RMX Web Clients must be opened (one for each MCU) by entering the IP Address of each MCU. If both conferences are running on the same MCU, only one RMX Web Client window is required.

When conferences are cascaded, the *Participant* list pane of each of the two conferences will display a linked icon ( ); a dial-in linked icon in the destination conference (Conference B) and a dial-out linked icon in the linked conference (Conference A).

The *Conferences* list panes in each of the two conferences will display a cascaded conference icon ( ) indicating that a conference running on the MCU is presently cascading with another conference running on the same or another MCU. The cascaded conference icon will be displayed for a short period of time and then
disappear.



Creating the Dial-out Link from a Conference Running on the MGC to the Conference Running on the RMX

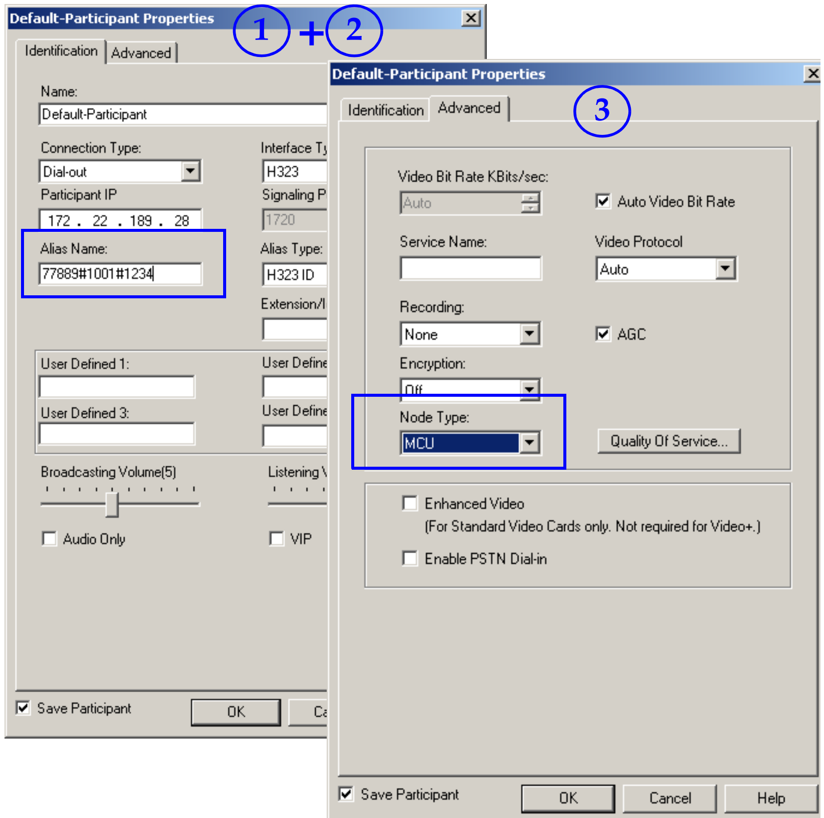
In the same way that the dial-out cascaded link is created in the RMX, you can create a dial-out participant in the MGC.

In the MGC Manager application, define a new participant as follows:

1 In the *Participant Properties* dialog box, enter a **Participant Name**, select **Dial-out** and **H.323**.

2 Define the **dialing string** as described in step 6 on page 5-23 (both methods are applicable).

3 In the *Advanced* tab's *Node Type* field, select **MCU**.



4 Click **OK**.

Cascading Conferences - H.239-enabled MIH Topology

H.239 Multi-Hierarchy (MIH) cascading is available to RMX users enabling them to run very large conferences on different MCUs in multiple levels of Master-Slave relationships using an H.323 connection.

Multi-Hierarchy (MIH) Cascading is implemented where the cascaded MCUs reside on different networks, whereas *Star Topology Cascading* requires that all cascaded MCUs reside on the same network.

MIH Cascading allows:

- Opening and using a content channel (H.239) during conferences.
- Full management of extremely large, distributed conferences.
- Connecting conferences on different MCUs at different sites.
- Utilizing the connection abilities of different MCUs, for example, different communication protocols, such as, serial connections, ISDN, etc.

- Significant call cost savings to be realized by having participants call local MCUs which in turn call remote MCUs, long distance.

> Although participants in MIH Cascading conferences can connect using H.323, SIP and ISDN, the MIH Cascading Links must connect via H.323.

MIH Cascading Levels

The cascading hierarchy topology can extend to up to four levels (Figure 5-9), where the most common configuration includes up to three levels.

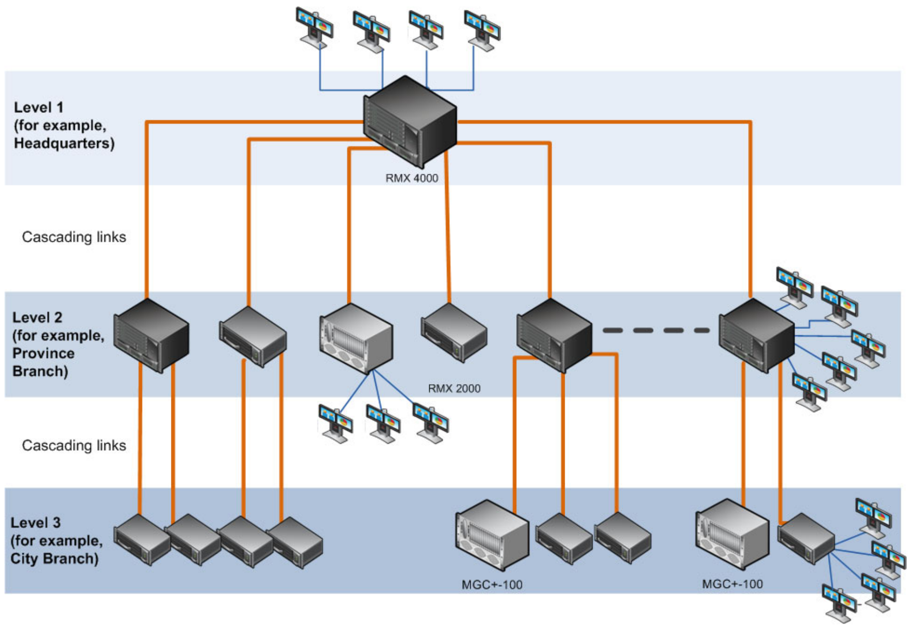


Figure 5-8 MIH Cascade - a Sample 3-Level Cascading Configuration

Cascading Topologies

The cascading hierarchy topology should be deployed according to the following guidelines:

- If an *RMX* is deployed on level 1 (recommended deployment):
  — Any *RMX* can be used on level 2, 3 and 4 (recommended deployment),
  — MGC version 9.0.4 can be used on level 2 and level 3,
  — *DST MCS 4000* and other MCUs can be deployed on levels 3 and 4.
- If an *MGC* is deployed on level 1:
  — *MGC* or *RMX* can be used on level 2,
  — *DST MCS 4000* and other MCUs can be deployed on levels 3 and 4.

- *DST MCS 4000 MCU*s connect as endpoints to the *RMX*s or *MGC*s on higher levels.

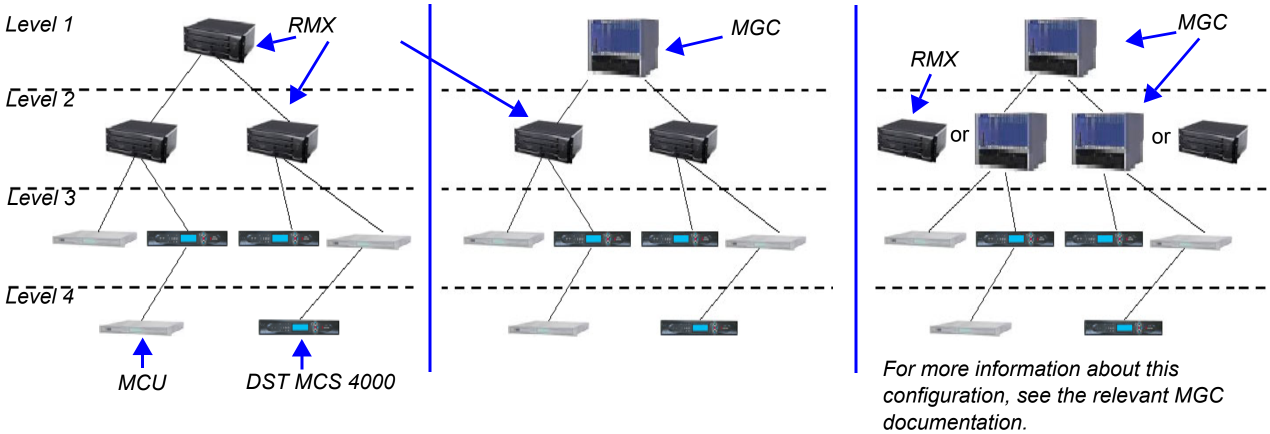


Figure 5-9 *MIH Cascade Levels*

MIH Cascading Guidelines in CP Licensing

Master - Slave Conferences

- It is recommended to have RMX systems at all levels to leverage the high quality video and content offered by the RMX.
- In *MIH Cascading* conferences, although there are multiple levels of Master and Slave relationships between conferences, the conference that runs on the MCU on level 1 of the hierarchy must be the Master for the entire cascading session. When an MGC is part of the cascading topology, it can be configured at any level if MGC Version 9.0.4 is installed, otherwise, it must be set as Level 1 MCU.
- Conferences running on MCUs on levels 2 and 3 and can be both Masters and Slaves to conferences running on MCUs on levels above and below them.
- All conferences running on MCUs on the lowest level in the configuration (for example, level 3 in a 3-level hierarchy configuration) are Slave conferences.
- When the DST MCS 4000 is on level 3 and acting as slave to level 2, the RMX on level 2 must dial out to it in order for the DST MCS 4000 to be identified as slave. The link between the two MCU (dial out participant) is defined as a standard participant and not as a cascading link.

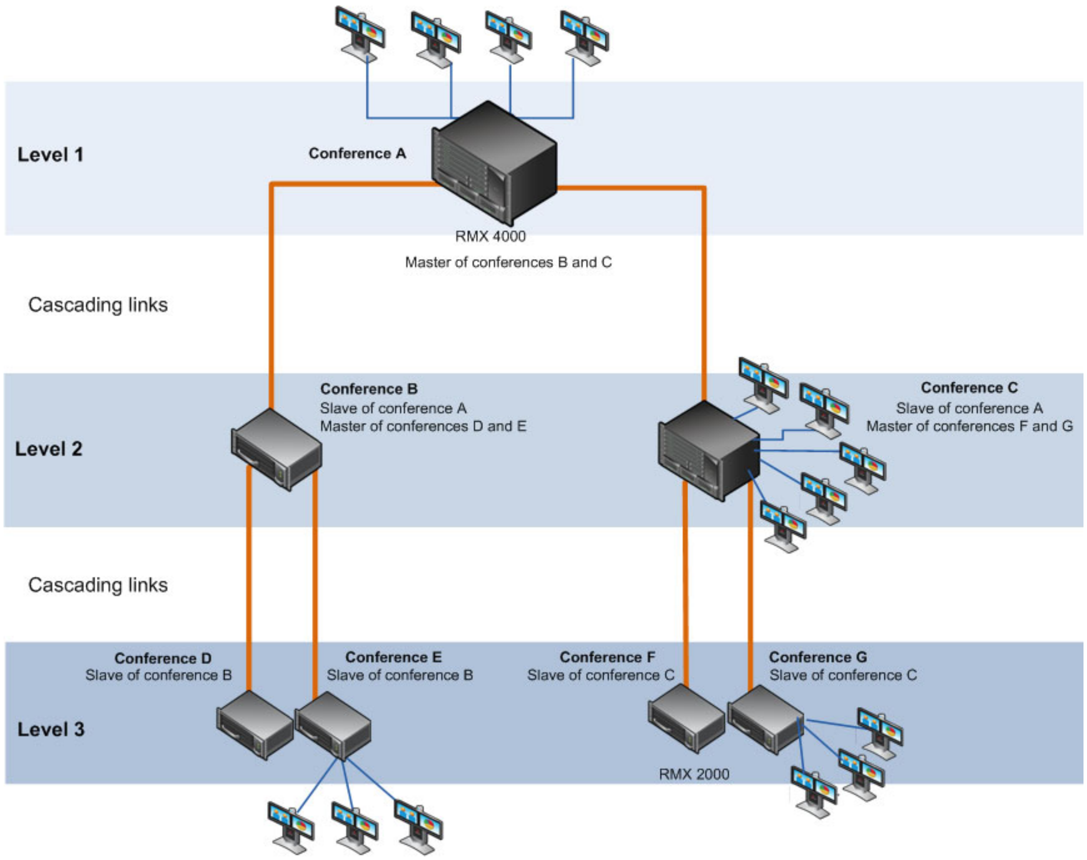


Figure 5-10MIH Cascading – Master-Slave Relationship

Video Session Mode, Line Rate and Video Settings

The types of MCUs, their position in the cascade topology and the endpoint capabilities (HD/CIF and H.263/H.264) determine the *Video Session Type* of the *MIH Cascading* conference.

- When creating a cascading link between two RMXs:
  — The RMXs operate in CP (Continuous Presence) mode.
  — DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences.
- When creating a cascading link between MGCs and RMXs:
  — If there are no MGCs on level 2, the MGCs can operate in either in CP or VSW (Video Switching) mode.
  — If there are MGCs on level 2, the MGCs can only operate in VSW mode.
  — MGC does not support H.264 High Profile, therefore when MGC is part of the Cascading topology, do not select *High Profil*e on the RMX system.
  — DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences.
- When creating a cascading link between two MGCs:
  — The MGCs must be configured to operate in VSW mode.

  For more details about the MGC to MGC connection, see the *MGC Manager User's Guide, Volume II, Chapter 1, "Ad Hoc Auto Cascading and Cascading Links"*.

- To enable the connection of the links between cascaded conferences, they must run at the same line rate.
- To enable Content sharing between the RMX and the MGC, the rate allocated to the content must be identical in both conferences. Make sure that the line rate set for both conferences, and the Content Settings (Graphics, Hi-res Graphics or Live video) are selected correctly to ensure the compatible rate allocation. For more details on the RMX rate allocation to the Content channel, see "*SIP BFCP Content Capabilities"* on page **4-3**.

The following table summarizes *Video Session Modes* line rate options that need to be selected for each conference in the cascading hierarchy according to the cascading topology:

Table 5-2 MIH Cascading – Video Session Mode and Line Rate

Topology	MCU Type	Video Session Type	Line Rate
Level 1	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 2	RMX		
Level 1	RMX	CP - CIF	768Kb/s, 2Mb/s
Level 2	RMX		
Level 1	RMX	CP	768Kb/s, 2Mb/s
Level 2	MGC	CP or VSW	
Level 1	MGC	CP - CIF 263	768 kb/s, 2Mb/s
Level 2	RMX	CP - CIF 264	
Level 1	MGC	VSW - HD	1.5Mb/s
Level 2	RMX	VSW HD	
Level 2	RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 3	RMX		
Level 2	MGC	VSW*	384 kbps, 768 kbps
Level 3	MGC		
Level 2	RMX	CP/VSW -HD	1.5Mb/s, 1Mb/s, 2Mb/s
Level 3	MCS 4000		
Level 2	RMX	CP - CIF	768kb/s, 2Mb/s
Level 3	MCS 4000		

* When MGC is on Level 3, Content cannot be shared between Level 2 and Level 3.

Video Layout in Cascading CP Conferences

Cascade links are treated as endpoints in CP conferences and are allocated resources according to "*Default Minimum Threshold Line Rates and Resource Usage Summary"* on page **3-12**. Cascaded links in 1x1 video layout are in SD resolution.

When cascading two conferences, the video layout displayed in the cascaded conference is determined by the selected layout in each of the two conferences. Each of the two conferences will inherit the video layout of the other conference in one of their windows.

In order to avoid cluttering in the cascaded window, it is advised to select appropriate video layouts in each conference before cascading them.

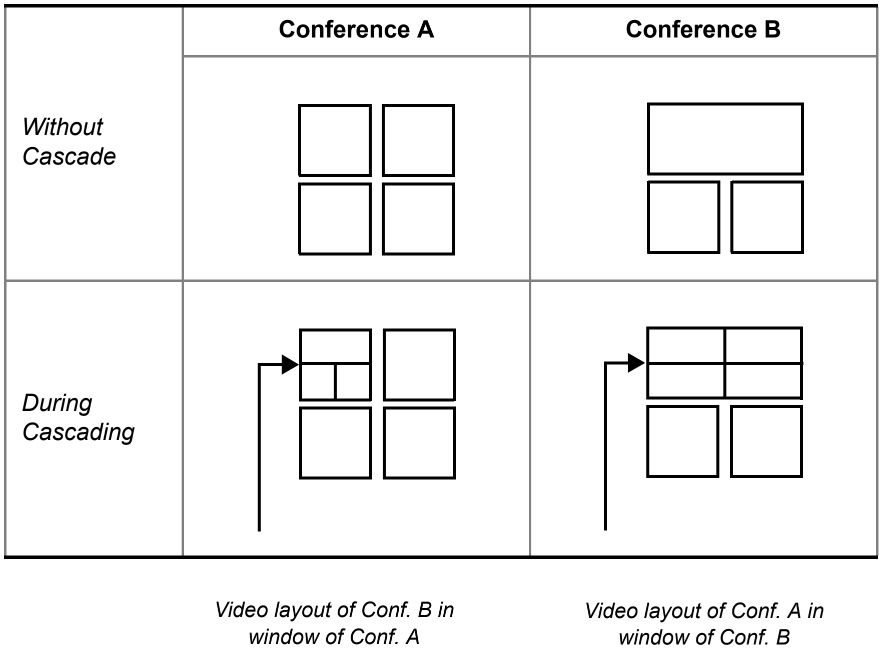


Figure 5-11 *Video Layouts in Cascaded Conferences*

Guidelines

To ensure that conferences can be cascaded and video can be viewed in all conferences the following guidelines are recommended:

- The same version installed on all MCUs participating the cascading topology
- The same license installed on all MCUs participating the cascading topology
- Same Conference Parameters are defined in the Profile of the conferences participating in the cascading topology
  - — Conference line rates should be identical
  - — Content rate should be identical
  - — Same encryption settings
- DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences
- DTMF forwarding is suppressed
- The video layout of the link is set to 1x1 by the appropriate system flag.

Flags controlling Cascade Layouts

- Setting the **FORCE_1X1_LAYOUT_ON_CASCADED_LINK _CONNECTION** *System Flag* to **YES** (default) automatically forces the cascading link to Full Screen (1x1) in CP conferences, hence displaying the speaker of one conference to a full window in the video layout of the other conference.

Set this flag to **NO** when cascading between an RMX and an MGC that is functioning as a Gateway, if the participant layouts on the MGC are not to be forced to 1X1.

- Setting the **AVOID_VIDEO_LOOP_BACK_IN_CASCADE** *System Flag* to **YES** (default) prevents the speaker's image from being sent back through the participant link from the cascaded conference. This can occur in cascaded conferences with conference layouts other than 1x1. It results in the speaker's own video image being displayed in the speaker's video layout.

  This option is supported with:

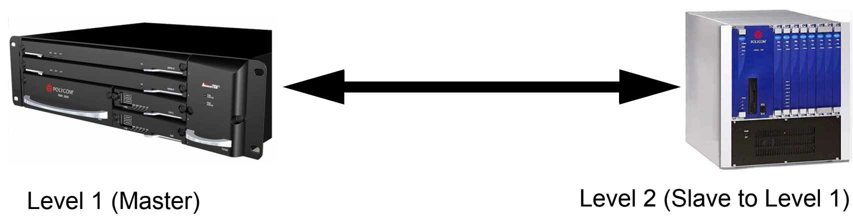
  — In *H.323, SIP* and *ISDN* environments.

  — For *Basic Cascading* of *Continuous Presence* and *Video Switched* conferences. If a *Master MCU* has two slave MCUs, participants connected to the slave MCUs will not receive video from each other.

  — Video resolution will be according to the *Resolution Configuration*, or *VSW* profile.

For more details on defining system flags, see "*Modifying System Flags"* on page **22-1**.

MGC to RMX Cascading



If MGC is running version 9.0.4, and RMX is running version 7.0.2 and higher, the RMX can be set as Master on level 1 and MGC as Slave on level 2.

MGC running versions other than 9.0.4 is always on level 1 and must be set as the Master MCU.

If the cascading topology includes additional MGCs as well as RMXs it is recommended to define Video Switching conferences for all the cascading conferences running on the MGC in the topology.

Two methods can be used to create the Cascading links between conferences running on the RMX and MGC:

- Method I - Establish the links by defining a dial-in and a dial-out participant in the Slave and Master conference (where the Master conference is created on the MCU on Level 1 and the Slave conference is created on the MCU on Level 2).
- Method II - Using a Cascading Entry Queue on either the MGC or the RMX depending on the dialing direction and the MCU Level. This is recommended when the RMX is on Level 1.

Method I

Depending on the dialing direction, the following procedures must be performed:

Table 5-3 Set up Procedures according to the Dialing Direction

Dialing Direction	RMX - Level 1	MGC - Level 2
MGC to RMX	Set the appropriate flags (done once only).	Set the appropriate flags (done once only).
	Define the conference setting and its line rate to be the same as the one set on the RMX.	Define the conference setting and its line rate to be the same as the one set on the MGC.
	Define the dial-in participant (Cascaded Link) with the calling number from the MGC. The alias that will be used to identify the dial-in participant can be the name of the calling slave conference. Set the Cascading option as Master.	Define the dial-out participant (Cascaded Link) to the conference running on the RMX. Set the dial-out alias to be the prefix of the MCU and the name of the master conference running on the RMX.
RMX to MGC	Set the appropriate flags (done once only)	Set the appropriate flags (done once only)
	Define the conference setting and its line rate to be the same as the one set on the RMX.	Define the conference setting and its line rate to be the same as the one set on the MGC.
	Define the dial-out participant (Cascaded Link). Set the dial-out alias to be the prefix of the MGC and the name of the slave conference running on the MGC. Set the Cascading option as Master.	Define the dial-in participant (Cascaded Link) to the conference running on the RMX. The alias that will be used to identify the dial-in participant can be the name of the calling slave conference.

For details on the participant definition on the RMX, see "*Creating a Cascade Enabled Dial-out/ Dial-in Participant Link"* on page **5-15**.

For a detailed description of the participant definition in the MGC, see the *MGC Manager User's Guide, Volume II, Chapter 1, Cascading Conferences*.

To enable Content sharing between the RMX and the MGC, the rate allocated to the content must be identical in both conferences. Make sure that the line rate set for both conferences, and the Content Settings (Graphics, Hi-res Graphics or Live video) are selected correctly to ensure the compatible rate allocation. For more details on the RMX rate allocation to the Content channel, see "*SIP BFCP Content Capabilities"* on page **4-3**.

Method II

Depending on the dialing direction, the following procedures must be performed:

Table 5-4 Set up Procedures according to the Dialing Direction

Dialing Direction	MGC Level 1	RMX 1500/2000/4000 Level 2
MGC to RMX	Set the appropriate flags (done once only).	Set the appropriate flags (done once only).
		Define the cascade-enabled Entry Queue, setting it as **Slave**.
	Define the conference setting and its line rate to be the same as the one set on the RMX.	Define the conference setting and its line rate to be the same as the one set on the MGC.
	Define the dial-out participant (Cascaded Link) to the conference running on the RMX.	
RMX to MGC	Set the appropriate flags (done once only)	Set the appropriate flags (done once only)
	Define the cascade-enabled Entry Queue.	
	Define the conference setting and its line rate to be the same as the one set on the RMX.	Define the conference setting and its line rate to be the same as the one set on the MGC.
		Define the dial-out participant (Cascaded Link) to the conference running on the MGC, setting the participant Cascade parameter to **Slave**.

Setting Flags on the RMX

When running conferences in mixed environment (RMX and MGC) there may be small differences between the line rates each MCU is sending. In the RMX, several flags must be set to ensure that these differences will not cause the cascaded link to connect as Secondary and that Content flows correctly between the cascaded conferences. This procedure is performed once per RMX.

To modify the flags:

1 In the RMX Web Client menu, click **Setup>System Configuration**.

2 In the *System Flags* dialog box, add the following new flags and values:

— **MIX_LINK_ENVIRONMENT=YES**
Setting this flag to YES will adjust the line rate of HD Video Switching conferences run on the RMX 1500/2000/4000 from 1920Kbps to 17897Kbps to match the actual rate of the HD Video Switching conference running on the MGC. In such case, the conference can include IP and ISDN participants.

— **IP_ ENVIRONMENT_LINK=NO**
Setting this flag to YES will adjust the line rate of HD Video Switching conferences run on the RMX 1500/2000/4000 from 1920Kbps to 18432Kbps to match the actual

rate of the IP Only HD Video Switching conference running on the MGC. In such case, the conference can include IP Only participants.

> If the flag MIX_LINK_ENVIRONMENT is set to YES, the *IP_LINK_ENVIRONMENT* flag must be set to NO.
> If the flag MIX_LINK_ENVIRONMENT is set to NO, the *IP_LINK_ENVIRONMENT* flag must be set to YES.

— **H263_ANNEX_T=YES (default)**
This flag enables/disables the use of Annex T with H263. Set it to NO if the endpoints connecting to the conference do not support this mode. In such a case, you must also change the MGC flag ENABLE_H239_ANNEX_T setting to NO.

— **FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION=YES** (default).
Set this flag to NO If the MGC is functioning as a Gateway and participant layouts on the other network are not to be forced to 1X1.

3 If the MGC is dialing the RMX and the cascaded link connects to the conference via the Cascade-enabled Entry Queue without being prompted for the conference password, set the flag to YES as follows:

— **ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD=YES**

4 Click **OK**.

5 Reset the MCU to apply the changes.

Setting Flags in the MGC

Flag setting is required to ensure the correct MCU behavior for cascading conferences. It is performed once per MCU.

To modify the flags:

1 In the MGC Manager, right-click the *MCU icon* and then click **MCU Utils>Edit "system.cfg"**.

2 In the **H264 Section**, ensure that the following flags are set to:

— **ENABLE_HD_SD_IN_FIXED_MODE=YES**
Setting this flag to YES enables H.264 Standard Definition (SD), High Definition (HD) and VSX 8000 (Version 8.0) support in Video Switching conferences.

— **H264_VSW_AUTO=NO**
Setting this flag to NO disables the highest common mechanism in H.264 and enables the selection of H.264 Video Protocol in fixed mode in Dual Stream Video Switching cascading conferences.

— **ENABLE_H239_ANNEX_T=YES**
This flag should be set to the same value (YES/NO) as the settings of the RMX flag H263_ANNEX_T

> To use MIH Cascade in the MGC, the Conference Numeric ID routing mode must be used. It is determined when the system.cfg flag in the GREET AND GUIDE/IVR section is set to QUICK_LOGIN_VIA_ENTRY_QUEUE=NO.

3 Click **OK**.

4 If you changed the flags, reset the MCU.

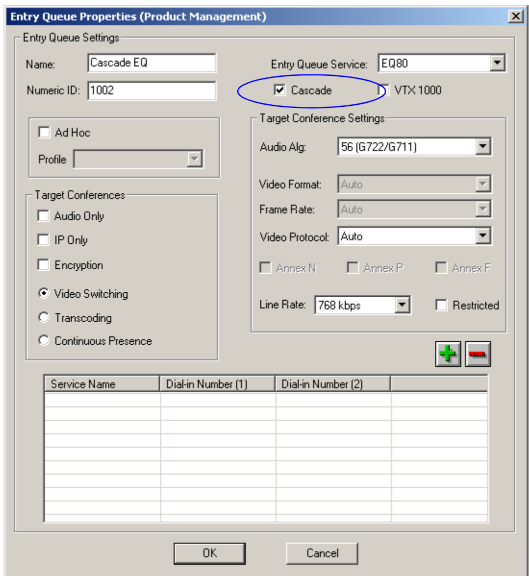
Method II - Defining the Cascading Entry Queue in the MGC

The Entry Queue definition on the MGC is required if the dialing is done from the RMX to the MGC.

1 In the MGC Manager, expand the *MCU tree*.

2 Right-click the *Meeting Rooms, Entry Queues and SIP Factories* icon and click **New Entry Queue**.

3 In the *New Entry Queue* dialog box, set the Entry Queue parameters and select the **Cascade** check box.



For more details on the definition of new Entry Queues refer to the *MGC Manager User's Guide, Volume II, Chapter 1, "Ad Hoc Auto Cascading and Cascading Links"*.

4 Click **OK**.

Creating the Dial-out Link between the Conference Running on the MGC and the Conference Running on the RMX

If the dialing is done from the MGC to the RMX, you need to define the cascaded link (dial-out participant) in the conference running on the MGC.

The dial-out string defined for the participant is the dialing string required to connect to the destination conference via the Cascade-enabled Entry Queue defined on the RMX hosting the destination cascaded conference. The dial-out participant can be defined on the MGC as template or assigned to the Meeting Room.

In the MGC Manager application, define a new participant as follows:

1 In the *Participant Properties - Identification* dialog box, enter a **Participant Name**

2 In the *Connection Type* field, select **Dial-out**.

3 In the *Interface Type* list field, select **H.323**.

4 There are two methods to define the dialing string to the other conference:

a Using the MCU's IP Address and the Alias string.

b Using only the Alias string (requires a gatekeeper).

Method A (If no gatekeeper is used):

In the *IP Address* field, enter the IP address of the **Signaling Host** of the RMX hosting the destination conference.

In the *Alias Name/Type* field, enter the ID of the cascade-enabled Entry Queue (EQ), the Conference ID and Password of the destination conference as follows:

EQ ID##Destination Conference ID##Password (Password is optional).

For Example: 1002##12001##1234

Cascade-enabled EQ ID *Destination Conference ID* *Password (optional)*

Method B (Using a gatekeeper):

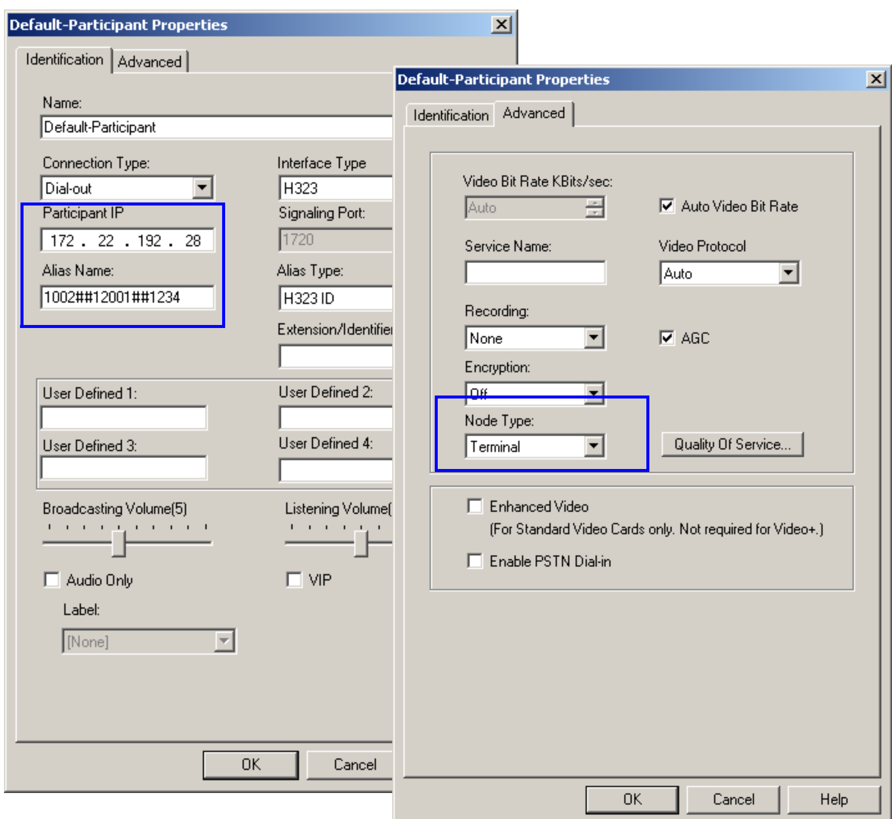
In the *Alias Name* field, enter the Prefix of MCU B, EQ ID, Destination Conference ID, and Password, as follows:

MCU Prefix EQ ID##Conference ID##Password (Password is optional)

For Example: 9251002##12001##1234

MCU Prefix as registered in the gatekeeper *Cascade-enabled EQ ID* *Conference ID* *Password (optional)*

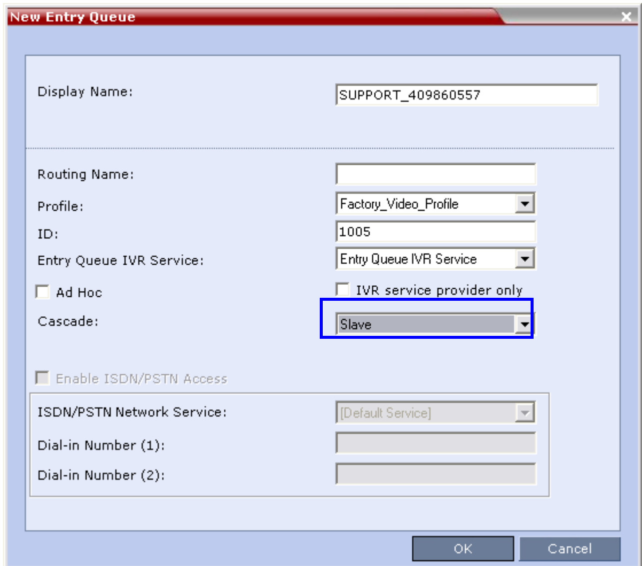
5 Click the *Advanced* tab and in the *Node Type* field, select **Terminal**.



6 Click **OK**.

Defining the Cascade Enabled Entry Queue on the RMX

If the dialing is done from the conference running on the MGC that is the Master MCU, a Cascade-enabled Entry Queue must be defined on the RMX setting it as **Slave**.



For more details, see RMX to RMX Cascading.

Defining the Cascading Conferences

The table below lists the line rates and the video settings that should be used when defining the conferences on the MGC. The same line rates should be selected when defining the Conference Profiles on the RMX, as well as whether the conference is HD Video Switching. However, the video settings will be automatically selected by the system.

Table 5-5 *Recommended Conference Line Rates for Cascaded Conferences*

Topology	Video Session Mode	Conference Line Rate
MGC ↓ RMX	MGC - CIF 263 RMX - CIF 264 CP	768Kb/s, 2Mb/s
	MGC - HD VSW RMX - HD VSW	1.5Mb/s

In addition, the conference running on the MGC should be set as **Meet Me Per Conference** and select the **H.239** option in the *Dual Stream Mode* field. *For more details on conference definition on the MGC, refer to the MGC Manager User's Guide, Volume I, Chapter 5.*

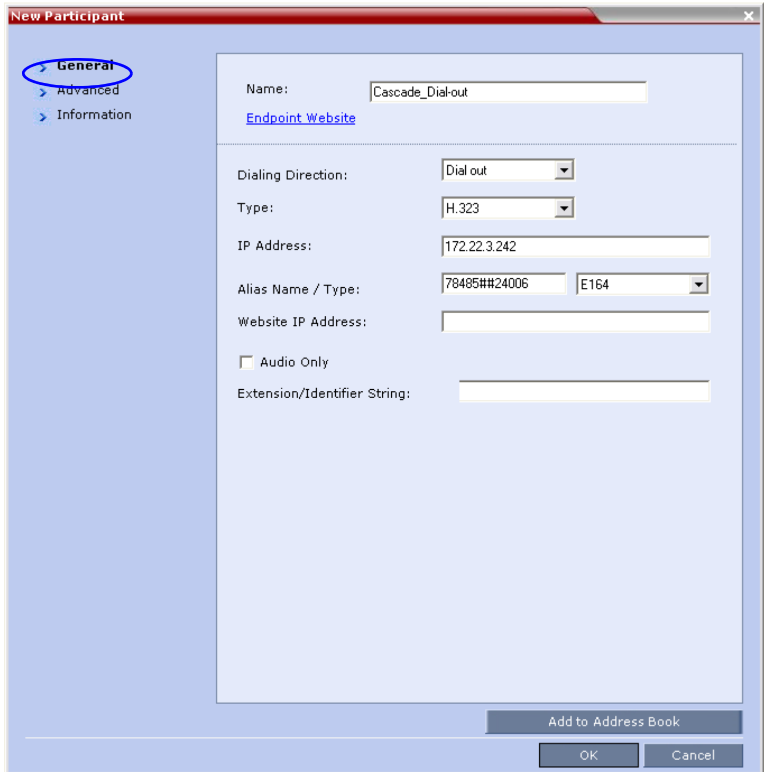
Defining the Dial-out Participant on the RMX

If the dialing is done from a conference running on the RMX to the conference running on the MGC, the dial-out participant is defined in the conference running on the RMX, setting the *Cascade* field to **Slave**. This participant dials the Cascade-enabled Entry Queue defined on the MGC.

1 Display the list of participants in the linked conference (Slave conference).

2 In the *Participant List* pane, click the **New Participant** () button.

The *New Participant - General* dialog box is displayed.



3 In the *Name* field, enter a participant name.

4 In the *Dialing Direction* field, select **Dial-out**.

5 In the *Type* list field, verify that **H.323** is selected.

6 There are two methods to define the dialing string:

A Using the MCU's IP Address and the Alias string.

B Using only the Alias string (requires a gatekeeper).

Method A (If no gatekeeper is used):

In the *IP Address* field, enter the IP address of the MGC hosting the destination conference (Master conference).

In the *Alias Name/Type* field, enter the ID of the cascade-enabled Entry Queue (EQ), the Conference ID and Password of the destination conference (Master Conference) as follows:

`EQ ID##Destination Conference ID##Password` (Password is optional).

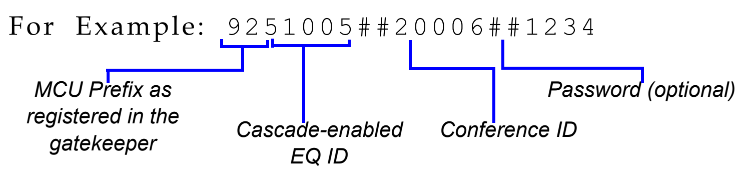
For Example: 1005##20006##1234

Cascade-enabled EQ ID — *Destination Conference ID* — *Password (optional)*

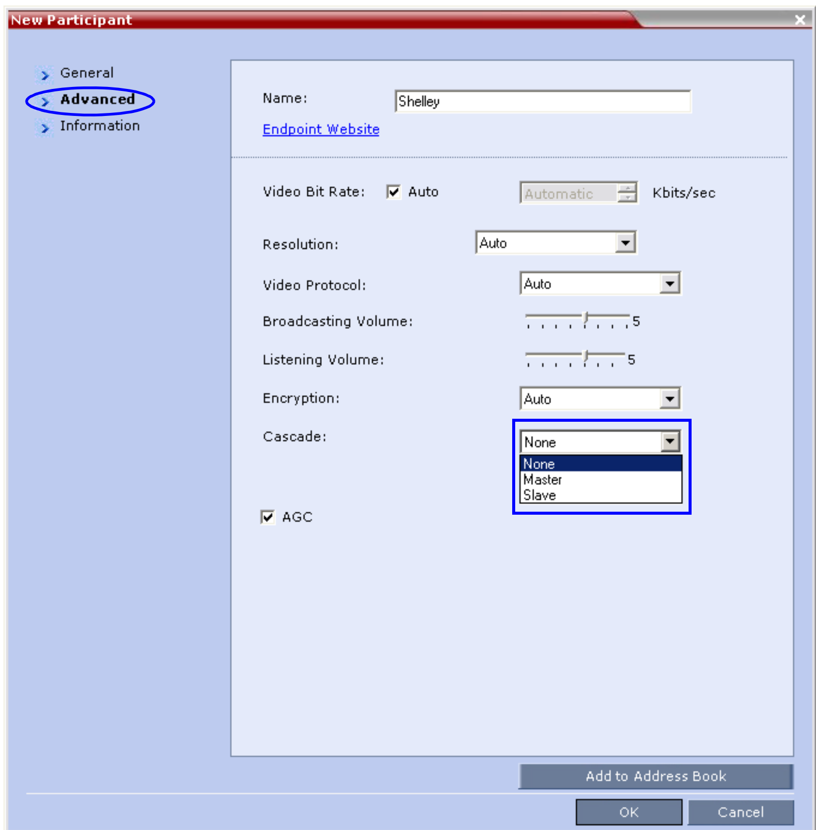
Method B (Using a gatekeeper):

In the *Alias Name* field, enter the MGC Prefix as registered in the gatekeeper, EQ ID, Destination Conference ID, and Password, as follows:

`MGC Prefix EQ ID##Conference ID##Password` (Password is optional)



7 Click the *Advanced* tab and in the *Cascade* field, select the **Slave** option.



8 Click **OK**.

The cascade-enabled dial-out link is created and the system automatically dials out to connect the participant to the local conference, as well as the destination conference on the MGC.

6

Meeting Rooms

A Meeting Room is a conference saved on the MCU in passive mode, without using any of the system resources. A Meeting Room is automatically activated when the first participant dials into it. Meeting Rooms can be activated as many times as required. Once activated, a Meeting Room functions as any ongoing conference.

The Meeting Room conferencing Mode is determined by the Profile assigned to it.

In SVC Conferencing Mode, dial-in is available as follows:

- AVC-capable endpoints (participants) can only connect to an AVC Meeting Room. When dialing into SVC Only Meeting Room the calls fail.
- SVC endpoints support both AVC and SVC video protocols. When dialing into SVC Only conferences, they connect as SVC endpoints. When dialing into AVC Only conferences, they connect as AVC endpoints.

In AVC Conferencing Mode, ISDN/PSTN participants can dial-in directly to a Meeting Room without connection through an Entry Queue. Up to two numbers can be defined per conference provided that they are from the same *ISDN/PSTN Network Service*. When a dial-in number is allocated to a Meeting Room, the number cannot be deleted nor can the *ISDN/PSTN Network Service* be removed. The dial-in number must be communicated to the ISDN or PSTN dial-in participants.

In AVC Conferencing Mode, dial-out participants can be connected to the conference automatically, or manually. In the automatic mode the system calls all the participants one after the other. In the manual mode, the RMX user or meeting organizer instructs the conferencing system to call the participant. Dial-out participants must be defined (mainly their name and telephone number) and added to the conference. This mode can only be selected at the conference/Meeting Room definition stage and cannot be changed once the conference is ongoing.

A Meeting Room can be designated as a Permanent Conference. For more information see "*Permanent Conference"* on page **4-80**.

The maximum of number of Meeting Rooms that can be defined is:

- RealPresence Collaboration Server (RMX) 1500/2000 — 1000
- RealPresence Collaboration Server (RMX) 4000 — 2000

The system is shipped with four default Meeting Rooms as shown in Table 6-1.

Table 6-1 *Default Meeting Rooms List*

Meeting Room Name	ID	Default Line Rate
Maple_Room	1001	384 Kbps
Oak_Room	1002	384 Kbps
Juniper_Room	1003	384 Kbps

Table 6-1 *Default Meeting Rooms List*

Meeting Room Name	ID	Default Line Rate
Fig_Room	1004	384 Kbps

Meeting Rooms List

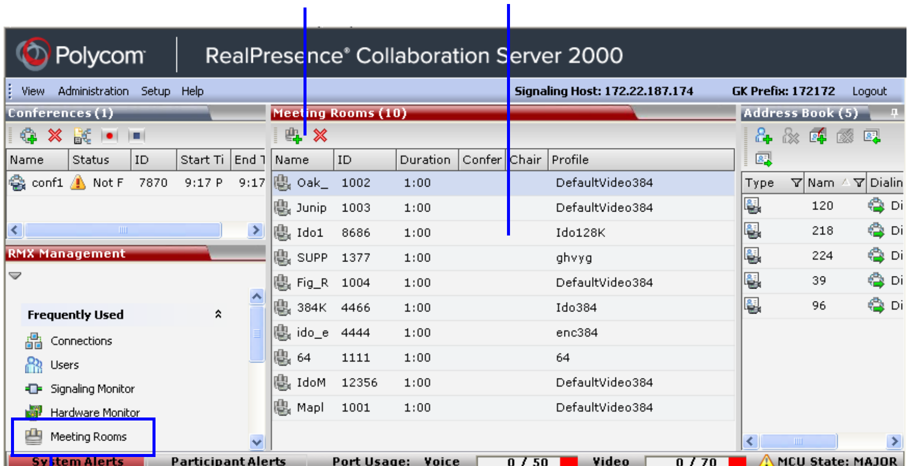
Meeting Rooms are listed in the *Meeting Room* list pane.

To list Meeting Rooms:

>> In the *RMX Management* pane, in the *Frequently Used* list, click the **Meeting Rooms** button .

The *Meeting Rooms List* is displayed.

Meeting Room Toolbar *Meeting Room List*



Access to Meeting Rooms

An active Meeting Room becomes an ongoing conference and is monitored in the same way as any other conference.

The *Meeting Room List* columns include:

Table 6-2 *Meeting Rooms List Columns*

Field	Description	
Display Name	Displays the name and the icon of the Meeting Room in the *RMX Web Client*.	
Display Name (cont.)	 (green)	An active video Meeting Room that was activated when the first participant connected to it.
	 (gray)	A passive video Meeting Room that is waiting to be activated.

Table 6-2 *Meeting Rooms List Columns (Continued)*

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>Routing Name</td><td colspan="2">The ASCII name that registers conferences, Meeting Rooms, Entry Queues and SIP Factories in the various gatekeepers and SIP Servers. In addition, the Routing Name is also:
• The name that endpoints use to connect to conferences.
• The name used by all conferencing devices to connect to conferences that must be registered with the gatekeeper and SIP Servers.</td></tr>
<tr><td>ID</td><td colspan="2">Displays the Meeting Room ID. This number must be communicated to H.323 conference participants to enable them to dial in.</td></tr>
<tr><td>Duration</td><td colspan="2">Displays the duration of the Meeting Room in hours using the format HH:MM (default 01:00).</td></tr>
<tr><td>Conference Password</td><td>The password to be used by participants to access the Meeting Room. If blank, no password is assigned to the conference. This password is valid only in conferences that are configured to prompt for a conference password in the IVR Service.</td><td rowspan="2">The RMX can be configured to automatically generate conference and chairperson passwords when these fields are left blank.
For more information, see the "Automatic Password Generation Flags” on page 22-45.</td></tr>
<tr><td>Chairperson Password</td><td>Displays the password to be used by the users to identify themselves as Chairpersons. They are granted additional privileges. If left blank, no chairperson password is assigned to the conference. This password is valid only in conferences that are configured to prompt for a chairperson password.</td></tr>
<tr><td>Profile</td><td colspan="2">Displays the name of the Profile assigned to the Meeting Room. For more information, see "Conference Profiles” on page 2-1.</td></tr>
<tr><td>SIP Registration</td><td colspan="2">The status of registration with the SIP server:
• Not configured - Registration with the SIP Server was not enabled in the Conference Profile assigned to this conferencing Entity. In Multiple Networks configuration, If one service is not configured while others are configured and registered, the status reflects the registration with the configured Network Services. The registration status with each SIP Server can be viewed in the Properties - Network Services dialog box of each conferencing entity.
When SIP registration is not enabled in the conference profile, the RMX's registering to SIP Servers will each register with an URL derived from its own signaling address. This unique URL replaces the non-unique URL, dummy_tester, used in previous versions.
• Failed - Registration with the SIP Server failed. This may be due to incorrect definition of the SIP server in the IP Network Service, or the SIP server may be down, or any other reason the affects the connection between the RMX or the SIP Server to the network.
• Registered - the conferencing entity is registered with the SIP Server.
• Partially Registered - This status is available only in Multiple Networks configuration, when the conferencing entity failed to register to all the required Network Services if more than one Network Service was selected.</td></tr>
</table>

Meeting Room Toolbar & Right-click Menu

The Meeting Room toolbar and right-click menus provide the following functionality:

Table 6-3 Meeting Room Toolbar and Right-click Menus

Toolbar button	Right-click menu	Description
	*New Meeting Room*	Select this button to create a new Meeting Room.
	*Delete Meeting Room*	Select any Meeting Room and then click this button to delete the Meeting Room.

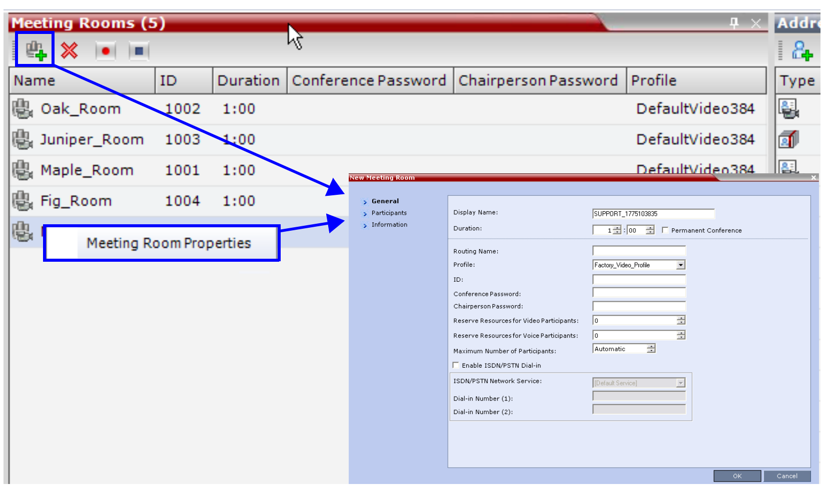
Dial out to participants assigned to a Meeting Room will only start when the dial in participant who has activated it has completed the connection process and the Meeting Room has become an ongoing conference.

Creating a New Meeting Room

To create a new meeting room:

>> In the *Meeting Rooms* pane, click the **New Meeting Room**  button *or* right-click an empty area in the pane and then click **New Meeting Room**.

The *New Meeting Room* dialog box is displayed.



The definition procedure is the same as for the new conference (with the exception of *Reserved Resources* for *Audio* and *Video* participants).

For more information, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide, "Starting an AVC Conference from the Conferences Pane"* on page **3-13**.

Microsoft Lync users can connect an RMX Meeting Room to a conference running on the Microsoft A/V MCU. This allows RMX Lync users to connect with a conference in progress on the A/V MCU and be an active participant in the conference.

For more information, see "*Connecting an MCU Meeting Room to a Microsoft AV-MCU Conference"* on page **H-62**.

7

Entry Queues, Ad Hoc Conferences and SIP Factories

Entry Queues

> Entry Queues are supported in AVC Conferencing Mode only.

An Entry Queue (EQ) is a special routing lobby to access conferences. Participants connect to a single-dial lobby and are routed to their destination conference according to the Conference ID they enter. The Entry Queue remains in a passive state when there are no callers in the queue (in between connections) and is automatically activated once a caller dials its dial-in number.

The maximum of number of Entry Queues that can be defined is:

- RealPresence Collaboration Server (RMX) 1500 — 40
- RealPresence Collaboration Server (RMX) 2000 — 40
- RealPresence Collaboration Server (RMX) 4000 — 80

The parameters (bit rate and video properties) with which the participants connect to the Entry Queue and later to their destination conference are defined in the Conference Profile that is assigned to the Entry Queue. For example, if the Profile Bit Rate is set to 384 Kbps, all endpoints connect to the Entry Queue and later to their destination conference using this bit rate even if they are capable of connecting at higher bit rates.

An *Entry Queue IVR Service* must be assigned to the Entry Queue to enable the voice prompts guiding the participants through the connection process. The Entry Queue IVR Service also includes a video slide that is displayed to the participants while staying in the Entry Queue (during their connection process).

Different Entry Queues can be created to accommodate different conferencing parameters (by assigning different Profiles) and prompts in different languages (by assigning different *Entry Queue IVR Services*).

For more information, see "*IVR Services"* on page **17-1**.

The Entry Queue can also be used for Ad Hoc conferencing. If the Ad Hoc option is enabled for the Entry Queue, when the participant enters the target conference ID the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID.

For more information about Ad Hoc conferencing, see "*Ad Hoc Conferencing"* on page **7-12**.

An Entry Queue can be designated as Transit Entry Queue to which calls with dial strings containing incomplete or incorrect conference routing information are transferred.

For more information, see "*Transit Entry Queue"* on page **7-6**.

To enable ISDN/PSTN participants to dial in to the Entry Queue, an ISDN/PSTN dial-in number must be assigned to the Entry Queue. Up to two dial-in numbers can be assigned to each Entry Queue. The dial-in numbers must be allocated from the dial-in number range defined in the ISDN/PSTN Network Service. You can allocate the two dial-in numbers from the same ISDN/PSTN Network Service or from two different ISDN/PSTN Network Services. The dial-in number must be communicated to the ISDN or PSTN dial-in participants.

The Entry Queue can also be used as part of the Gateway to Polycom® Distributed Media Application™ (DMA™) 7000 solution for connecting Audio only PSTN, ISDN, SIP and H.323 endpoints to DMA™ 7000.

For more information, see Appendix D, *"Gateway to Polycom® DMA™ 7000"* .

Default Entry Queue properties

The system is shipped with a default Entry Queue whose properties are:

Table 7-1 *Default Entry Queue Properties*

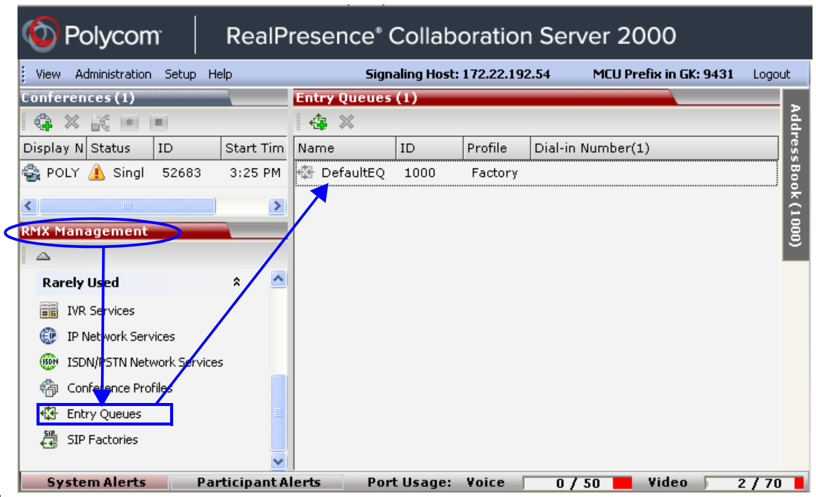
Parameter	Value
Display Name	DefaultEQ The user can change the name if required.
Routing Name	DefaultEQ The default *Routing Name* cannot be changed.
ID	1000
Profile name	Factory-Video-Profile. Profile Bit Rate is set to 384 Kbps.
Entry Queue Service	Entry Queue IVR Service. This is default Entry Queue IVR Service shipped with the system and includes default voice messages and prompts in English.
Ad Hoc	Enabled
Cascade	None (Disabled)
Enable ISDN/PSTN Access	Disabled. You can modify the properties of this Entry Queue to enable ISDN/PSTN participants to dial-in to a conference. Up to two dial-in numbers can be assigned.

Defining a New Entry Queue

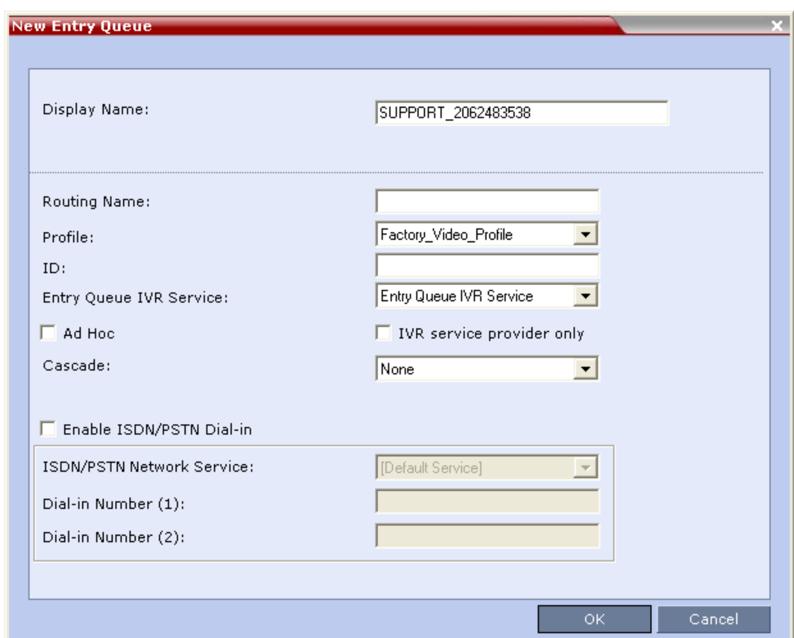
You can modify the properties of the default Entry Queue and define additional Entry Queues to suit different conferencing requirements.

To define a new Entry Queue:

1 In the *RMX Management - Rarely Used* pane, click **Entry Queues**.



2 In the *Entry Queues* list pane, click the **New Entry Queue**  button.
The *New Entry Queue* dialog box opens.



3 Define the following parameters:

Table 7-2: Entry Queue Definitions Parameters

Option	Description
Display Name	The Display Name is the conferencing entity name in native language character sets to be displayed in the RMX Web Client. In conferences, Meeting Rooms, Entry Queues and SIP factories the system automatically generates an ASCII name for the *Display Name* field that can be modified using Unicode encoding. • English text uses ASCII encoding and can contain the most characters (length varies according to the field).
Display Name (cont.)	• European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII). Maximum field length in ASCII is 80 characters. If the same name is already used by another conference, Meeting Room or Entry Queue, the RMX displays an error message requesting you to enter a different name.
Routing Name	Enter a name using ASCII text only. If no *Routing Name* is entered, the system automatically assigns a new name as follows: • If an all ASCII text is entered in *Display Name*, it is used also as the *Routing Name.* • If any combination of Unicode and ASCII text (or full Unicode text) is entered in *Display Name*, the *ID* (such as Conference ID) is used as the *Routing Name.*
Profile	Select the Profile to be used by the Entry Queue. The default Profile is selected by default. This Profile determines the Bit Rate and the video properties with which participants connect to the Entry Queue and destination conference. In Ad Hoc conferencing it is used to define the new conference properties. To connect to a Video Switching conference via Entry Queue, the Profile assigned to the Entry Queue must be set to Video Switching. It is recommended to use the same profile for both the destination conference and Entry Queue.
ID	Enter a unique number identifying this conferencing entity for dial in. Default string length is 4 digits. If you do not manually assign the ID, the MCU assigns one after the completion of the definition. The ID String Length is defined by the flag NUMERIC_CONF_ID_LEN in the System Configuration.
Entry Queue IVR Service	The default Entry Queue IVR Service is selected. If required, select an alternate Entry Queue IVR Service, which includes the required voice prompts, to guide participants during their connection to the Entry Queue.

Table 7-2: Entry Queue Definitions Parameters (Continued)

Option	Description
Ad Hoc	Select this check box to enable the Ad Hoc option for this Entry Queue.
IVR Service Provider Only	Select this check box to designate this Entry Queue as a special Entry Queue that provides IVR Services to SIP calls on behalf of the DMA. The IVR service provider only EntryQueue does not route the SIP calls to a target conference. Instead the DMA handles the call. For more details, see "*IVR Provider Entry Queue (Shared Number Dialing)"* on page **7-7**.
Cascade	Set this field to **None** for all Entry Queues other than cascading. If this Entry Queue is used to connect dial-in cascaded links, select **Master** or **Slave** depending on the Master/Slave relationship in the Cascading topology. Set this field to *Master* if: • The Entry Queue is defined on the MCU on level 1 and the dialing is done from level 2 to level 1. • The Entry Queue is defined on the MCU on level 2 and the dialing is done from level 3 to level 2. Set this field to *Slave* if the Entry Queue is defined on the MCU on level 2 (Slave) and the dialing is done from MCU level 1 to level 2.
Enable ISDN/PSTN Access	Select this check box to allocate dial-in numbers for ISDN/PSTN connections. To define the first dial-in number using the default ISDN/PSTN Network Service, leave the default selection. When the Entry Queue is saved on the MCU, the dial-in number will be automatically assigned to the Entry Queue. This number is taken from the dial-in numbers range in the default ISDN/PSTN Network Service.
ISDN/PSTN Network Service	The default Network Service is automatically selected. To select a different ISDN/PSTN Network Service in the service list, select the name of the Network Service.
Dial-in Number (1)	Leave this field blank to let the system automatically assign a number from the selected ISDN/PSTN Network Service. To manually define a dial-in number, enter a required number from the dial-in number range defined for the selected Network Service.
Dial-in Number (2)	By default, the second dial-in number is not defined. To define a second-dial-in number, enter a required number from the dial-in number range defined for the selected Network Service.

4 Click **OK**.

The new *Entry Queue* is added to the *Entry Queues* list.

Listing Entry Queues

To view the list of Entry Queues:

>> In the *RMX Management - Rarely Used* pane, click **Entry Queues**.

The *Entry Queues* are listed in the *Entry Queues* pane.

You can double-click an Entry Queue to view its properties.

Modifying the EQ Properties

To modify the EQ:

>> In the *Entry Queues* pane, either double-click or right-click and select **Entry Queue Properties** of the selected *Entry Queue* in the list.

The Entry Queue Properties dialog box is displayed. All the fields may be modified except **Routing Name**.

Transit Entry Queue

A *Transit Entry Queue* is an Entry Queue to which calls with dial strings containing incomplete or incorrect conference routing information are transferred.

IP Calls are routed to the *Transit Entry Queue* when:

- A gatekeeper is not used, or where calls are made directly to the RMX's *Signaling IP Address*, with incorrect or without a Conference ID.
- When a gatekeeper is used and only the prefix of the RMX is dialed, with incorrect or without a Conference ID.
- When the dialed prefix is followed by an incorrect conference ID.

When no *Transit Entry Queue* is defined, all calls containing incomplete or incorrect conference routing information are rejected by the RMX.

In the *Transit Entry Queue*, the *Entry Queue IVR Service* prompts the participant for a destination conference ID. Once the correct information is entered, the participant is transferred to the destination conference.

Setting a Transit Entry Queue

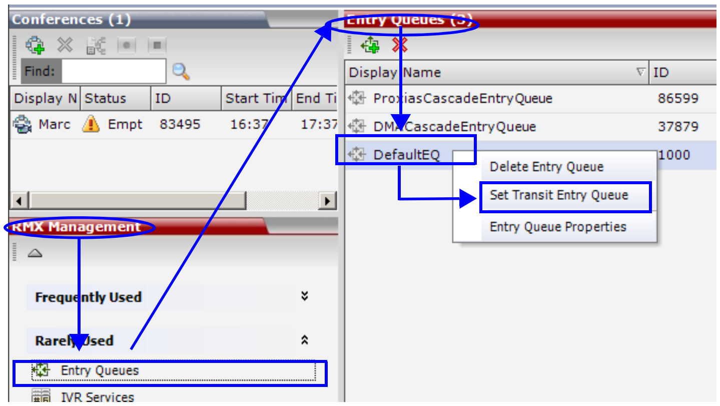
The RMX factory default settings define the *Default Entry Queue* also as the *Transit Entry Queue*. You can designate another Entry Queue as the *Transit Entry Queue*.

Only one *Transit Entry Queue* may be defined per RMX and selecting another Entry Queue as the *Transit Entry Queue* automatically cancels the previous selection.

To designate an Entry Queue as Transit Entry Queue:

1 In the *RMX Management - Rarely Used* pane, click **Entry Queues**.

2 In the *Entry Queues* list, right-click the Entry Queue entry and then click **Set Transit Entry Queue**.



The Entry Queue selected as *Transit Entry Queue* is displayed in bold.

To cancel the Transit Entry Queue setting:

1 In the *RMX Management - Rarely Used* pane click **Entry Queues**.

2 In the *Entry Queues* list, right-click the *Transit Entry Queue* entry and then click **Cancel Transit Entry Queue**.

IVR Provider Entry Queue (Shared Number Dialing)

In an environment that includes a DMA, the RMX Entry Queue can be configured to provide the IVR Services on behalf of the DMA to SIP endpoints. It displays the Welcome Slide, plays the welcome message and retrieves the destination conference ID that is entered by the participant using DTMF codes.

To enable this feature, a special Entry Queue that is defined as *IVR Service Provider only* is created. This Entry Queue does not forward calls to conferences running on the RMX and its main functionality is to provide IVR services.

Call Flow

The SIP participant dials the DMA Virtual Entry Queue number, for example 1000@dma.polycom.com.

The DMA forwards the SIP call to the RMX, to a special Entry Queue that is configured as *IVR Service Provider Only*. The participant is prompted to enter the conference ID using DTMF codes.

Once the participant enters the conference ID, the conference ID is forwarded to the DMA, enabling the DMA to connect the SIP endpoint to the destination conference or create a new conference and connect the participant to that conference.

Guidelines

- An Entry Queue defined as IVR service provider only does not route the SIP call to a target conference and it cannot be used to rout calls on the RMX. In such a configuration, the DMA handles the calls. Therefore, normal Entry Queues must be defined separately.

- *Operator Assistance* must be disabled in the IVR Service assigned to this Entry Queue.
- Only the conference ID prompts should be configured. Other prompts are not supported in *IVR Service Provider Only* configuration.
- PSTN, ISDN, H.323 calls to this Entry Queue are rejected.
- The DMA must be configured to locate the *IVR Service Provider Only* Entry Queue on the RMX. To locate the Entry Queue the DMA requires the Entry Queue's ID number and the RMX Central Signaling IP address (xxx.xx.xxx.xx).

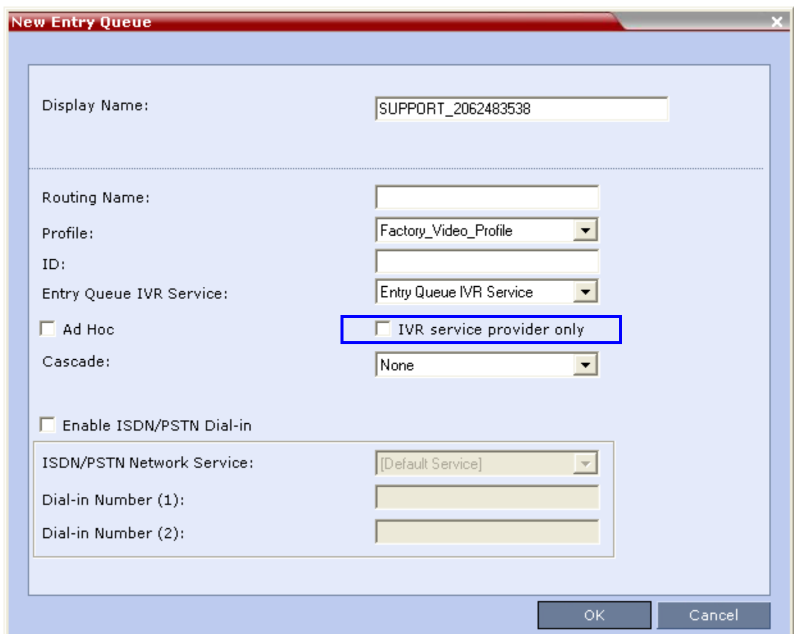
RMX Configuration

Entry Queue IVR Service

If required, create a special Entry Queue IVR Service in which the *Operator Assistance* option is disabled and only the *Conference ID* prompts are enabled.

Entry Queue

>> In the *New Entry Queue* dialog box, select **IVR Service Provider Only.**



— Enter the Entry Queue ID that will be used by the DMA to forward the SIP calls to this Entry Queue.

— Select the special Entry Queue IVR Service if one was created.

— *Ad Hoc*, *Cascade* and *Enable ISDN/PSTN Dial-in* options should not be selected with this type of Entry Queue.

SIP Factories

A SIP Factory is a conferencing entity that enables SIP endpoints to create Ad Hoc conferences. The system is shipped with a default SIP Factory, named DefaultFactory.

When a SIP endpoint calls the SIP Factory URI, a new conference is automatically created based on the Profile parameters, and the endpoint joins the conference.

The SIP Factory URI must be registered with the SIP server to enable routing of calls to the SIP Factory. To ensure that the SIP factory is registered, the option to register *Factories* must be selected in the Default IP Network Service.

The maximum of number of SIP Factories that can be defined is:

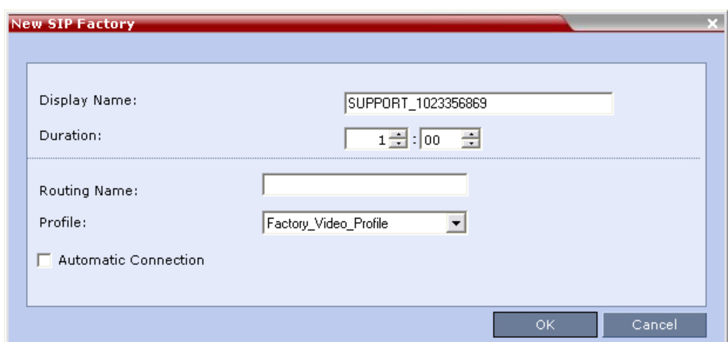
- RealPresence Collaboration Server (RMX) 1500 — 40
- RealPresence Collaboration Server (RMX) 2000 — 40
- RealPresence Collaboration Server (RMX) 4000 — 80

Creating SIP Factories

To create a new SIP Factory:

1 In the *RMX Management - Rarely Used* pane, click **SIP Factories**.

2 In the *SIP Factories* list pane, click the **New SIP Factory**  button.
The *New Factory* dialog box opens.



3 Define the following parameters:

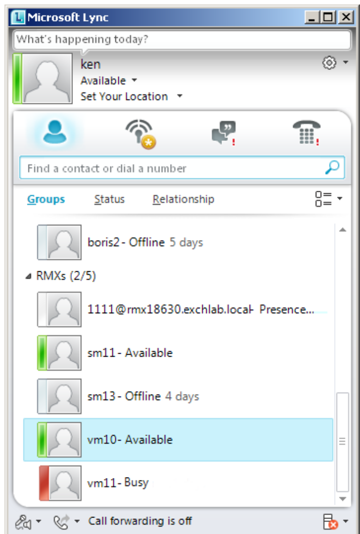
Table 7-3: New Factory Properties

Option	Description
Display Name	Enter the SIP Factory name that will be displayed. The Display Name is the conferencing entity name in native language character sets to be displayed in the RMX Web Client. In conferences, Meeting Rooms, Entry Queues and SIP factories the system automatically generates an ASCII name for the *Display Name* field that can be modified using Unicode encoding. • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII). Maximum field length in ASCII is 80 characters. If the same name is already used by another conference, Meeting Room or Entry Queue, the RMX displays an error message requesting you to enter a different name.
Routing Name	The *Routing Name* is defined by the user, however if no *Routing Name* is entered, the system will automatically assign a new name when the Profile is saved as follows: • If an all ASCII text is entered in *Display Name*, it is used also as the *Routing Name.* • If any combination of Unicode and ASCII text (or full Unicode text) is entered in *Display Name*, the *ID* (such as Conference ID) is used as the *Routing Name.*
Profile	The default Profile is selected by default. If required, select the conference Profile from the list of Profiles defined in the MCU. A new conference is created using the parameters defined in the Profile.
Automatic Connection	Select this check box to immediately accept the conference creator endpoint to the conference. If the check box is cleared, the endpoint is redirected to the conference and then connected.

4 Click **OK**.
The new SIP Factory is added to the list.

SIP Registration & Presence for Entry Queues and SIP Factories

Entry Queues and *SIP Factories* can be registered with *SIP* servers. This enables *Office Communication Server* or *LYNC* server client users to see the availability status (*Available, Offline,* or *Busy*) of these conferencing entities and to connect to them directly from the *Buddy List*.



Guidelines

- The *Entry Queue* or *SIP Factory* must be added to the *Active Directory* as a *User*.
- *SIP Registration* must be enabled in the *Profile* assigned to the *Entry Queue* or *SIP Factory*. For more information see *Step* of "*Defining New Profiles"* on page **2-18**.

Monitoring Registration Status

The *SIP* registration status can be viewed in the *Entry Queue* or *SIP Factory* list panes.

The following statuses are displayed:

- **Not configured** - *Registration* with the *SIP* Server was not enabled in the *Conference Profile* assigned to the *Entry Queue* or *SIP Factory*.

When SIP registration is not enabled in the conference profile, the RMX's registering to SIP Servers will each register with an URL derived from its own signaling address. This unique URL replaces the non-unique URL, dummy_tester, used in previous versions.

- **Failed** - *Registration* with the *SIP Server* failed.
  This may be due to incorrect definition of the *SIP* server in the *IP Network Service*, or the *SIP Server* may be down, or any other reason the affects the connection between the RMX or the *SIP Server* to the network.
- **Registered** - the conferencing entity is registered with the *SIP Server*.
- **Partially Registered** - This status is available only in *Multiple Networks* configuration, when the conferencing entity failed to register to all the required *Network Services* if more than one *Network Service* was selected for *Registration*.

Ad Hoc Conferencing

The Entry Queue can also be used for Ad Hoc conferencing. If the Ad Hoc option is enabled for the Entry Queue, when the participant enters the target conference ID the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID. The conference parameters are based on the Profile linked to the Entry Queue. As opposed to Meeting Rooms, that are predefined conferences saved on the MCU, Ad Hoc conferences are not stored on the MCU. Once an Ad Hoc conference is started it becomes an ongoing conference, and it is monitored and controlled as any standard ongoing conference.

An external database application can be used for authentication with Ad Hoc conferences. The authentication can be done at the Entry Queue level and at the conference level. At the Entry Queue level, the MCU queries the external database server whether the participant has the right to create a new conference. At the conference level the MCU verifies whether the participant can join the conference and if the participant is the conference chairperson. The external database can populate certain conference parameters.

For more information about Ad Hoc conferencing, see *Appendix D, "Ad Hoc Conferencing and External Database Authentication"* on page **D-1**.

Gateway to Polycom® Distributed Media Application™ (DMA™) 7000

Gateway to Polycom® Distributed Media Application™ (DMA™) 7000 enables audio only PSTN, ISDN (video endpoints using only their audio channels), SIP and H.323 calls to connect to the Polycom DMA 7000 via gateway sessions running on the RMX. Each RMX conference acting as a gateway session includes one connection to the endpoint and another connection to the DMA. The DMA 7000 enables load balancing and the distribution of multipoint calls on up to 10 Polycom RMX media servers.

As part of this solution, the RMX acts as a gateway for the DMA that supports H.323 calls. The PSTN, ISDN or SIP endpoint dials the virtual Meeting Room on the DMA via a special Entry Queue on the RMX.

For more information, see *"Dialing to Polycom® DMA™ 7000"* on page **19-25**.

8

Address Book

The Address Book stores information about the people and businesses you communicate with. The Address Book stores, among many other fields, IP addresses, phone numbers and network communication protocols used by the participant's endpoint. By utilizing the Address Book you can quickly and efficiently assign or designate participants to conferences. Groups defined in the Address Book help facilitate the creation of conferences. Participants can be added to the Address Book individually or in Groups.

The maximum of number of Address Book entries that can be defined on the RMX 1500/2000/4000 is 4000.

When using the Polycom CMA Global Address Book, all entries are listed.

The Address Book can be organized into a multi-level hierarchical structure. It can be used to mirror the organizational layout of the enterprises and it is especially suitable for large-scale enterprises with a considerable number of conference participants and organizational departments and divisions. Groups in the Address Book can contain sub-groups or sub-trees, and individual address book participant entities.

The Address Book provides flexibility in arranging conference participants into groups in multiple levels and the capabilities to add groups or participants, move or copy participants to multiple groups within the address book, and use the address book to add groups and participants to a conference or *Conference Template*.

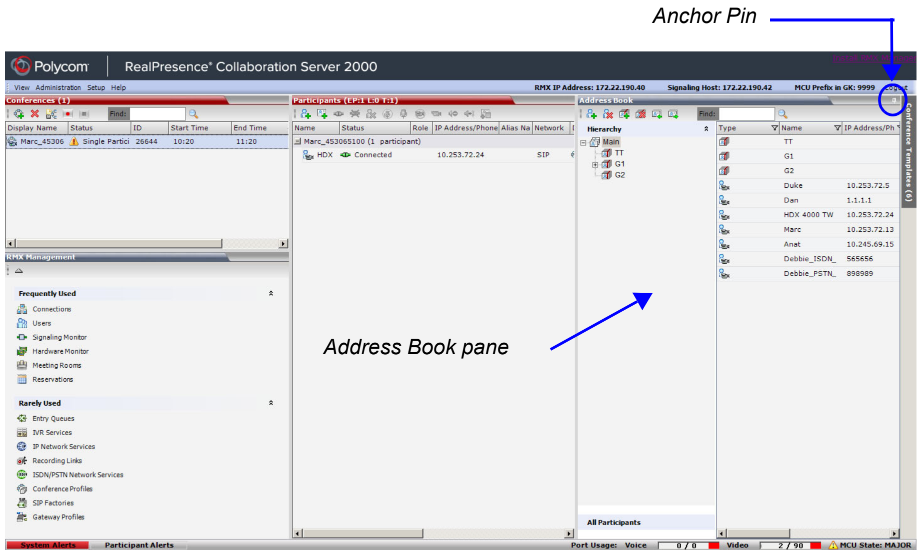
Importing and exporting of Address Books enables organizations to seamlessly distribute up-to-date Address Books to multiple RMX units. It is not possible to distribute Address Books to external databases running on applications such as *Polycom's ReadiManager (SE200)* or *Polycom CMA*. External databases can run in conjunction with RMX units, but must be managed from the external application. For example, new participants cannot be added to the external database from the RMX Web Client. To enable the RMX to run with an external database such as Polycom CMA, the appropriate system configuration flags must be set.

For more information, see "*Modifying System Flags"* on page **22-1**.

> Integration with Polycom CMA Global Address Book is supported. For more information, see "*Integrating the Polycom CMA™ Address Book with the RMX"* on page **8-23**. Integration with the *SE200* GAB (Global Address Book) is not supported.

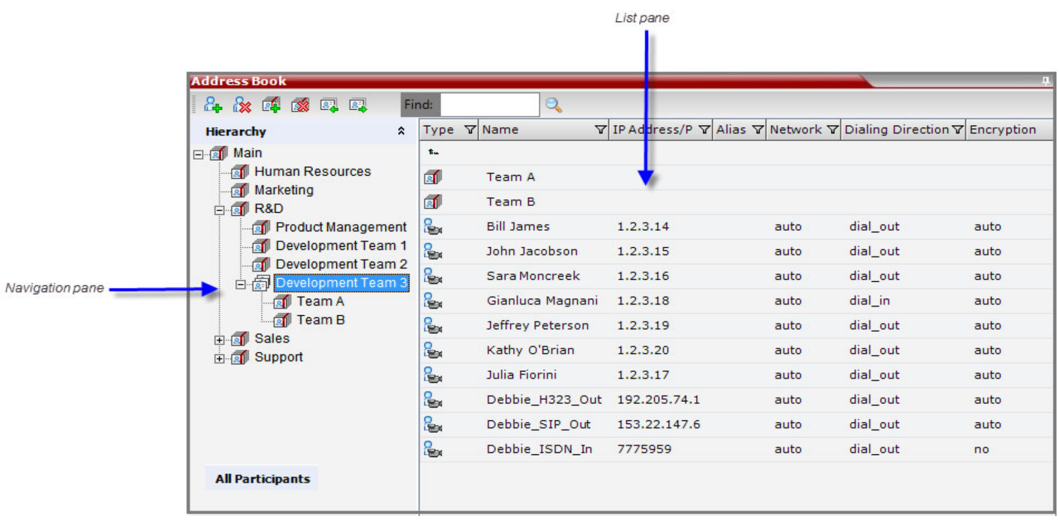
Viewing the Address Book

You can view the participants currently defined in the Address Book. The first time the *RMX Web Client* is accessed, the *Address Book* pane is displayed.



The *Address Book* contains two panes:

- *Navigation pane* - contains the hierarchical tree and *All Participants* list
- *List pane* - displays the list of all the members of the selected group and sub-groups.



The *Navigation pane* of the *Address Book* contains the following types of lists:

- **Hierarchical** — displays a multi-level hierarchical tree of groups and participants. Double-clicking a group on the navigation pane displays the group participants and sub-groups in the *List* pane.
- **All Participants** — double-clicking this selection displays the single unique entity of all the participants in a single level. When adding a participant to a group, the system adds a link to the participant's unique entity that is stored in the All Participants list. The same participant may be added to many groups at different levels, and all these

participant links are associated with the same definition of the participant in the *All Participants* list. If the participant properties are changed in one group, they will be changed in all the groups accordingly.

Displaying and Hiding the Group Members in the Navigation Pane

The currently selected group, whose group members are displayed in the Address Book List pane is identified by a special icon .

To expand the group to view the group members:

>> Double-click the group name or click the **Expand** button.

The address book entities and sub-groups of the group is displayed in the right group list pane. You can drill down the sub-group to view address book entities in the sub-group.

To move up to the next level and view the members in the upper level:

>> Double-click the **navigation arrow** button in the group members pane.

To collapse a group:

>> Double-click the group name or click the **Collapse** button.

Participants List Pane Information

The *Participants List* pane displays the following information for each participant:

Table 8-1 *Docked Address Book List Columns*

Field/Option	Description
Type	Indicates whether the participant is a video ( ) or voice ( ).
Name	Displays the name of the participant.
IP Address/Phone	Enter the IP address of the participant's endpoint. • For H.323 participant define either the endpoint IP address or alias. • For SIP participant define either the endpoint IP address or the SIP address. **Note:** This field is removed from the dialog box when the ISDN/PSTN protocol is selected.
Network	The network communication protocol used by the endpoint to connect to the conference: *H.323*, *SIP* or *ISDN/PSTN* .

Table 8-1 *Docked Address Book List Columns (Continued)*

Field/Option	Description
Dialing Direction	*Dial-in* – The participant dials in to the conference. *Dial-out* – The RMX dials out to the participant.
Encryption	Displays whether the endpoint uses encryption for its media. The default setting is *Auto*, indicating that the endpoint must connect according to the conference encryption setting.

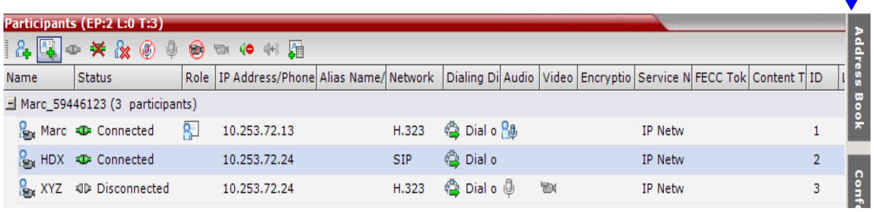
For information on adding and modifying participants in the Address Book, see "*Managing the Address Book"* on page 8-7.

Displaying and Hiding the Address Book

The Address Book can be hidden it by clicking the anchor pin ( ) button in the pane header. The *Address Book* pane closes and a tab is displayed at the right edge of the screen.

>> Click the tab to re-open the *Address Book*.

Click tab to open Address Book



Adding Participants from the Address Book to Conferences

You can add individual participants or a group of participants from the Address Book to a conference.

Adding Individual Participants from the Address Book to Conferences

You can add a participant or multiple participants to a new conference, ongoing conferences, or to *Conference Templates* by using the drag-and-drop operation.

Multiple selection of group levels is not available.

To add a participant to a new conference or an ongoing conference:

1 In the *Address Book Navigation* pane, select the group from which to add participants.

2 In the *Address Book List* pane, select the participant or participants you want to add to the conference.

3 Click and hold the left mouse button and drag the selection to the Participants pane of the conference.

   The participants are added to the conference.

Adding a Group from the Address Book to Conferences

You can add a group of participants to a new conference, ongoing conferences, or to *Conference Templates* by using the drag-and-drop operation.

To add a group to a new conference or an ongoing conference:

1 In the *Address Book Navigation* pane, select the group you want to add to the conference.

2 Click and hold the left mouse button and drag the selection to the *Participants* pane of the conference.

   The participants in the group level and all sub-levels are added to the conference.

Participant Groups

A group is a predefined collection of participants. A group provides an easy way to manage clusters of participants that are in the same organizational structure and to connect a combination of endpoints to a conference. For example, if you frequently conduct conferences with the marketing department, you can create a group called “Marketing Team” that contains the endpoints of all members of the marketing team.

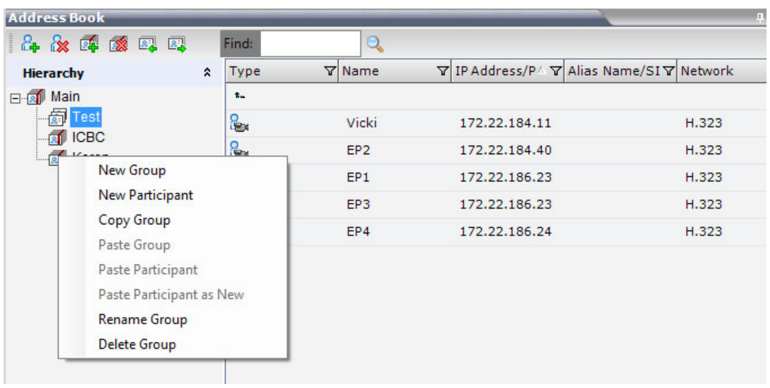
Groups can contain participants and sub-groups. You can define up to ten levels in the “Main” group.

Managing Groups in the Address Book

To manage the groups in the Address Book:

1 In the *Address Book Navigation* pane, right-click the group you want to manage.

The *Groups* menu is displayed.



2 Select one of the following actions:

Table 8-2 *Groups Drop-down Menu Actions*

Action	Description
New Group	Creates a new group within the current group.
New Participant	Adds a new participant within the current group.
Copy Group	Copies the current group to be pasted as an additional group.
Paste Group	Places the copied group into the current group. The group name of the copied group is defined with “*Copy*” at the end of the group name. This action is only available after a **Copy Group** action has been implemented.
Paste Participant	Places the copied participant into the current selected group. This action is available after a **Copy** or **Cut** action was activated when selecting a single participant or multiple participants.
Paste Participant as New	Pastes as a new participant into the selected group. This paste action adds “*Copy*” at the end of the participant name. This action is only available after a **Copy** action was activated for a single participant.
Rename Group	Renames the group name.

Table 8-2 Groups Drop-down Menu Actions (Continued)

Action	Description
Delete Group	Deletes the group and all of its members. This action displays a message requesting confirmation to delete the group and all members connected with the group.

Additionally, you can drag a group from one location in the Address Book to another location, moving the group and all its members, including sub-groups, to its new location using the drag-and-drop operation. Moving a group to a new location can be done in the navigation pane or the list pane.

To drag a group from a location in the address book to another location:

1 Select the group you want to move.

2 Click and hold the left mouse button and drag the selection to the new location. The new location can be either the "Main" root level or another group level.

   The group and all its members (participants and groups) are moved to the new address book location.

Managing the Address Book

Guidelines

- The multi-level *Address Book* can only be used in a local configuration on the RMX. The hierarchical structure cannot be implemented with the *Global Address Book* (GAB).
- Up to ten levels can be defined in the hierarchical structure of the Address Book.
- The default name of the root level is "Main". The "Main" root level cannot be deleted but the root level name can be modified.
- Address Book names support multilingual characters.
- Participants in the *Address Book* can be copied to multiple groups. However, only one participant exists in the *Address Book*. Groups that contain the same participants refer to the same definition of the participant entity.

Adding a Participant to the Address Book

Adding participants to the Address Book can be performed by the following methods:

- Directly in the Address Book.
- Moving or saving a participant from an ongoing conference to the Address Book.

Only defined **dial-out** ISDN/PSTN participants can be added to the Address Book or ongoing conferences. ISDN/PSTN participants are added to the Address Book in the same manner that H.323 and SIP participants are added.

When adding dial-out participants to the ongoing conference, the system automatically dials out to the participants using the Network Service (ISDN/PSTN or IP) defined for the connection in the participant properties.

Adding a new participant to the Address Book Directly

You can add a new participant to the “Main” group or to a group in the *Address Book*. Additionally, you can add a participant from a new conference, ongoing conference, or *Conference Template*.

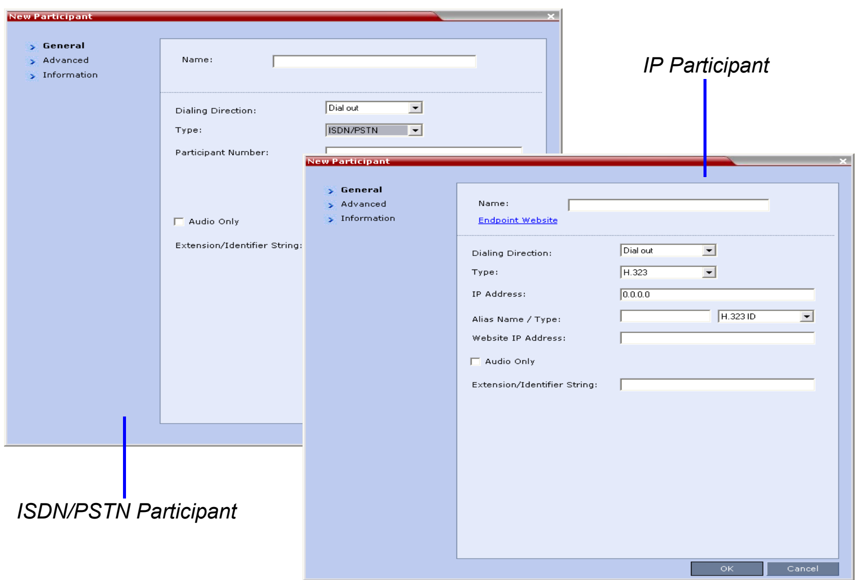
To add a new participant to the Address Book:

1 In the *Address Book - Navigation* pane, select the group to where you want to add the new participant.

2 Click the **New Participant** button ( ) or right-click the group to where you want to add the participant and select the **New Participant** option.

— Alternatively, click anywhere in the *List* pane and select the **New Participant** option.

The *New Participant - General* dialog box opens.



3 Define the following fields:

Table 8-3 New Participant – General Properties

Field	Description
Name	Enter the name of the participant or the endpoint as it will be displayed in the RMX Web Client. The *Name* field can be modified using Unicode encoding. • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. Maximum field length in ASCII is 80 characters. The maximum length of text fields varies according to the mixture of character sets used (Unicode and ASCII). This name can also become the endpoint name that is displayed in the video layout. For more details about endpoint (site) names, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide*, *"Text Indication in the Video Layout (AVC Only Conferencing)"* on page **3-34**". **Note:** This field is displayed in all tabs.
Endpoint Website (IP only)	Click the Endpoint Website hyperlink to connect to the internal website of the participant's endpoint. It enables you to perform administrative, configuration and troubleshooting activities on the endpoint. The connection is available only if the IP address of the endpoint's internal site is defined in the *Website IP Address* field.
Dialing Direction	Select the dialing direction: • ***Dial-in*** – The participant dials in to the conference. This field applies to IP participants only. • ***Dial-out*** – The MCU dials out to the participant. **Note:** • Dial-out is forced when defining an ISDN/PSTN participant.
Type	The network communication protocol used by the endpoint to connect to the conference: *H.323*, *SIP* or *ISDN/PSTN*. The fields in the dialog box change according to the selected network type.

Table 8-3 *New Participant – General Properties (Continued)*

Field	Description
IP Address **(H.323 and SIP Only)**	Enter the IP address of the participant's endpoint. • For H.323 participant define either the endpoint IP address or alias. • For SIP participant define either the endpoint IP address or the SIP address. For RMXs registered to a gatekeeper, the RMX can be configured to dial and receive calls to and from H.323 endpoints using the IP address in the event that the Gatekeeper is not functioning. For more information, see "*Gateway Calls"* on page **19-1**. **Note:** This field is hidden when the ISDN/PSTN protocol is selected.
Phone Number **(ISDN/PSTN Only)**	Enter the phone number of the ISDN/PSTN participant. **Note:** This field is only displayed when the ISDN/PSTN protocol is selected.
Alias Name/Type **(H.323 Only)**	If you are using the endpoint's alias and not the IP address, first select the type of alias and then enter the endpoint's alias: • H.323 ID (alphanumeric ID) • E.164 (digits 0-9, * and #) • Email ID (email address format, e.g. abc@example.com) • Participant Number (digits 0-9, * and #) **Note:** • Although all types are supported, the type of alias is dependent on the gatekeeper's capabilities. The most commonly supported alias types are H.323 ID and E.164. • This field is used to enter the Entry Queue ID, target Conference ID and Conference Password when defining a cascaded link. • This field is removed from the dialog box when the ISDN/PSTN protocol is selected.
SIP Address/Type **(SIP Only)**	Select the format in which the SIP address is written: • ***SIP URI*** - Uses the format of an E-mail address, typically containing a user name and a host name: *sip:*[*user]@[host]*. For example, sip:dan@polycom.com. • ***TEL URI*** - Used when the endpoint does not specify the domain that should interpret a telephone number that has been input by the user. Rather, each domain through which the request passes would be given that opportunity. For example, a user in an airport might log in and send requests through an outbound proxy in the airport. If the users enters "411" (this is the phone number for local directory assistance in the United States), this number needs to be interpreted and processed by the outbound proxy in the airport, and not by the user's home domain. In this case, tel: 411 is the correct choice. Note: This field is removed from the dialog box when the ISDN/PSTN protocol is selected.

Table 8-3 New Participant – General Properties (Continued)

Field	Description
Endpoint Website IP Address ***(IP only)***	Enter the IP address of the endpoint's internal site to enable connection to it for management and configuration purposes. This field is automatically completed the first time that the endpoint connects to the RMX. If the field is blank it can be manually completed by the system administrator. The field can be modified while the endpoint is connected
Audio Only	Select this check box to define the participant as a voice participant, with no video capabilities.
Extension/Identifier String	Dial-out participants that connect to an external device such as Cascaded Links or Recording Links may be required to enter a conference password or an identifying string to connect. Enter the required string as follows: [p]…[p][string] For example: pp4566# p - optional - indicates a pause of one second before sending the DTMF string. Enter several concatenated [p]s to increase the delay before sending the string. The required delay depends on the configuration of the external device or conference IVR system. String - enter the required string using the digits 0-9 and the characters * and #. The maximum number of characters that can be entered is identical to the H.323 alias length. If the information required to access the device/conference is composed of several strings, for example, the conference ID and the conference password, this information can be entered as one string, where pauses [p] are added between the strings for the required delays, as follows: [p]…[p][string][p]…[p] [string]... For example: p23pp*34p4566#
Extension/Identifier String (continued)	The RMX automatically sends this information upon connection to the destination device/conference. The information is sent by the RMX as DTMF code to the destination device/conference, simulating the standard IVR procedure.

4 Usually, additional definitions are not required and you can use the system defaults for the remaining parameters. In such a case, click **OK**.

To modify the default settings for advanced parameters, click the **Advanced** tab.

5 Define the following *Advanced* parameters:

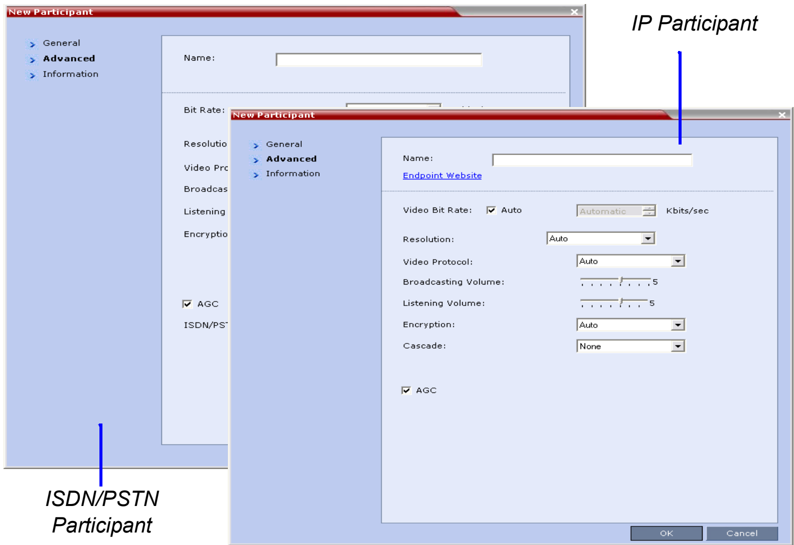


Table 8-4 *New Participant – Advanced Properties*

Field	**Description**
Video Bit Rate / Auto **(IP Only)**	The *Auto* check box is automatically selected to use the Line Rate defined for the conference. **Note:** This check box cannot be cleared when defining a new participant during an ongoing conference. To specify the video rate for the endpoint, clear this check box and then select the required video rate.
Video Protocol	Select the video compression standard that will be forced by the MCU on the endpoint when connecting to the conference: *H.261*, *H.263*, *H.264* or *RTV*. Select **Auto** to let the MCU select the video protocol according to the endpoint's capabilities.
Resolution	The *Auto* check box is automatically selected to use the Resolution defined for the conference. To specify the Resolution for the participant, select the required resolution from the drop-down menu.
Broadcasting Volume + Listening Volume	To adjust the volume the participant broadcasts to the conference or the volume the participant hears the conference, move the slider; each unit represents an increase or decrease of 3 dB (decibel). The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default connection value is 5.
Encryption	Select whether the endpoint uses encryption for its connection to the conference. **Auto** (default setting) indicates that the endpoint will connect according to the conference encryption setting.

Table 8-4 New Participant – Advanced Properties (Continued)

Field	Description
AGC	AGC (Auto Gain Control) mechanism regulates noise and audio volume by keeping the received audio signals of all participants balanced. Select this check box to enable the AGC mechanism for participants with weaker audio signals. **Notes:** • To be enable AGC, set the value of the ENABLE_AGC *System Flag* in *system.cfg* to be YES. The flag's default value is NO. • If the *System Flag* does not exist in the system, it must be manually added to the System Configuration. For more information see "*Modifying System Flags"* on page **22-1**. • Enabling AGC may result in amplification of background noise.
Cascaded Link ***(IP Only)***	If this participant is used as a link between conferences select: • **Slave**, if the participant is defined in a conference running on a Slave MCU. • **Master**, if the participant is defined in a conference running on the Master MCU. It enables the connection of one conference directly to another conference using an H.323 connection only. The conferences can run on the same MCU or different MCU's. For more information, see "*Enabling Cascading"* on page **5-21**.
ISDN/PSTN Network Service	Enables users to select the ISDN/PSTN network service.

6 To add general information about the participant, such as e-mail, company name, and so on, click the **Information** tab and type the necessary details in the **Info 1-4** fields. Text in the *info* fields can be added in Unicode format (length: 31 characters).

7 Click **OK**.

The new participant is added to the selected group in the address book.

Adding a Participant from an Ongoing Conference to the Address Book

You can add a participant to the Address Book directly from an ongoing conference.

When adding a participant to the address book from a new conference, *Participants* list of an ongoing conference or *Conference Template*, the participant is always added to the "Main" group.

To add a participant from the conference to the Address Book:

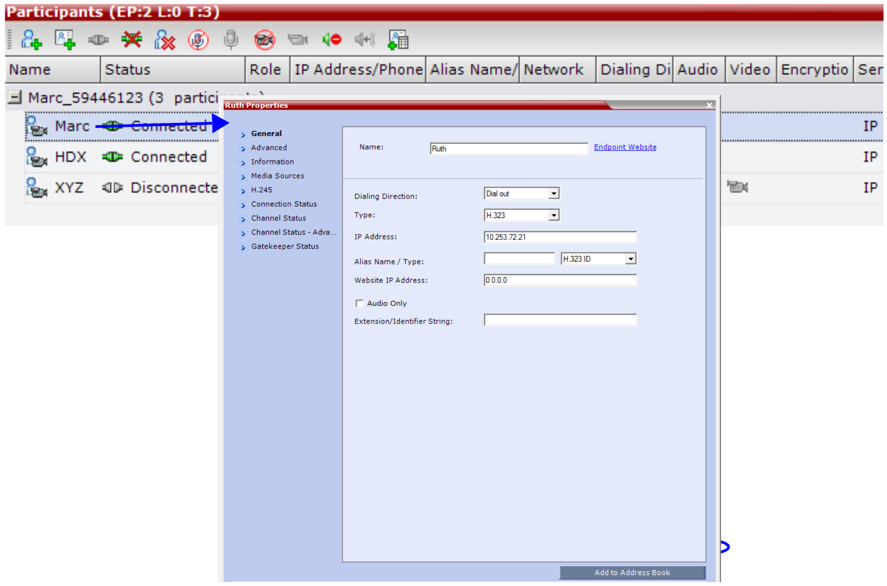
1 During an ongoing conference, select the participant in the *Participant* pane and either click the **Add Participant to Address Book** button ( ) or right-click and select **Add Participant to Address Book**.

The participant is added to the Address Book.

Alternatively, you could:

a Double-click the participant's icon or right-click the participant icon and click **Participant Properties**.

The *Participant Properties* window opens.



b Click the **Add to Address Book** button.

> If the participant name is already listed in the All Participants list, an error message is displayed. In such a case, change the name of the participant before adding the participant to the address book.

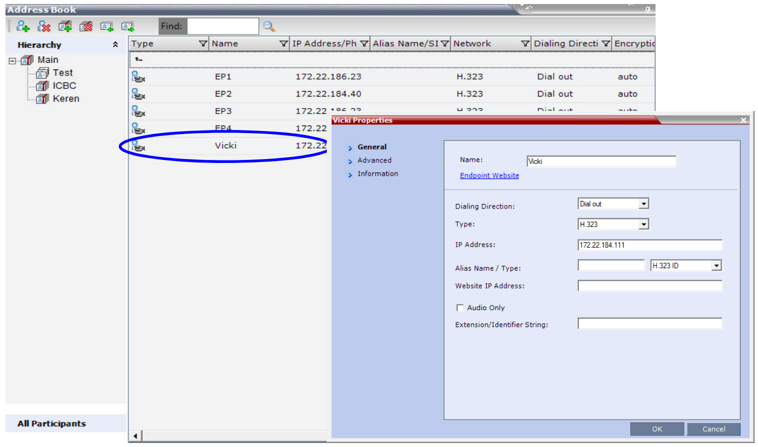
Modifying Participants in the Address Book

When required, you can modify the participant's properties.

To modify participant properties in the Address Book:

1. In the *Address Book - Navigation* pane, select the group to where the participant to modify is listed.

2 In the *Address Book - List* pane, double-click the participant's icon. The *Participant's Properties* window is displayed.



3 Modify the necessary properties in the window, such as dialing direction, communication protocol type, and so on. You can modify any property in any of the three tabs: *General*, *Advanced* and *Info*.

4 Click **OK**.

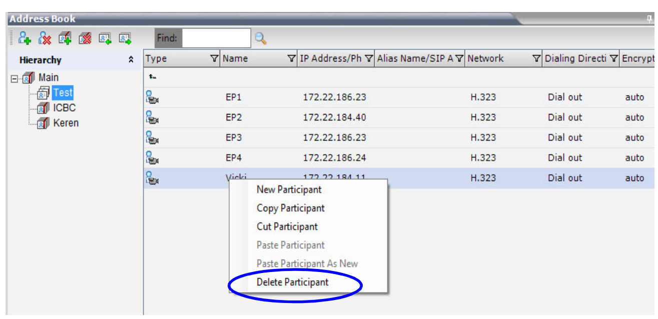
The changes to the participant's properties are updated.

Deleting Participants from the Address Book

To delete participants from the Address Book:

1 In the *Address Book - Navigation* pane, select the group where the participant to delete is listed.

2 In the *Address Book - List* pane, either select the participant to delete and then click the **Delete Participant** ( ) button, or right-click the participant icon and then click the **Delete Participant** option.



3 A confirmation message is displayed depending on the participant's assignment to groups in the address book:

a When the participant belongs to only one group: click **Yes** to permanently delete the participant from the address book.

b When the participant belongs to multiple groups, a message is displayed requesting whether to delete the participant from the *Address Book* or from the current selected group. Select:

- **Current group** to delete the participant from the selected group

- **Address Book** to permanently delete the participant from the address book (all groups).

Click **OK** to perform the delete operation or **Cancel** to exit the delete operation.

Copying or Moving a Participant

You can copy or move a participant from one group to another group using the **Copy**, **Cut**, and **Paste** options. A participant can belong to multiple groups. However, there is only one entity per participant. Groups that contain the same participants refer to the same definition of the participant entity. Alternatively, you can drag a participant from one location in the *Address Book* to another location, moving the participant to its new location using the drag-and-drop operation.

> The cut and copy actions are not available when selecting multiple participants.

To copy or move a participant to another group:

1. In the *Address Book - Navigation* pane, select the group from where to copy the participant.
2. In the *Address Book - List* pane, select the participant you want to copy.
3. Right-click the selected participant and select one of the following functions from the drop-down menu:

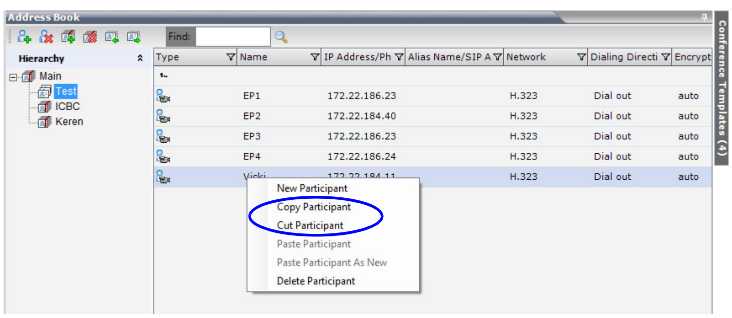


Table 8-5 Copy/Cut Functions

Function	Description
Copy Participant	Copies the participant to be pasted into an additional group.
Cut Participant	Moves the participant from the current group to a different group. Alternatively, you can move a participant to another location by dragging the participant to the new location.

4. In the *Address Book* navigation pane, navigate and select the group in which you want to paste the participant.

5 Right-click the selected group and click one of the following **Paste** functions from the drop-down menu:

Table 8-6 *Paste functions*

Function	Description
Paste Participant	Creates a link to the participant entity in the pasted location.
Paste Participant as New	Pastes as a new participant into the selected group. This paste action adds "*Copy*" to the end of the participant name.

The Paste functions are only available after a **Copy** or **Cut** action has been implemented.

To drag a participant from an address book group to another group:

1 Select the participant or participants you want to move.

2 Click and hold the left mouse button and drag the selection to the new group.

The participants are moved to the new address book group.

Searching the Address Book

You can search the *Address Book* for a participant's name or a group name only on the currently selected group/level.

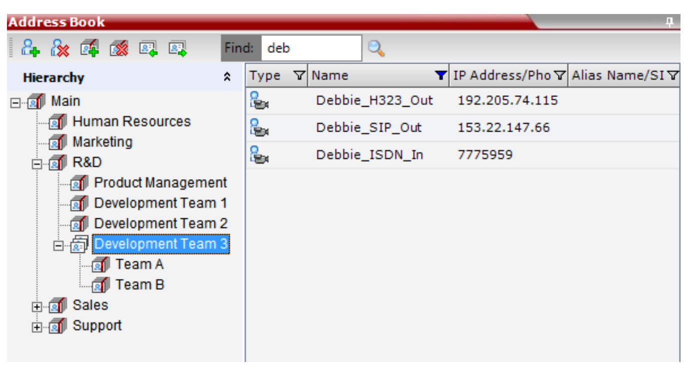
To search for participants or groups in the current selected level:

1 In the *Address Book Navigation* pane, select the group/level within to run the search.

2 In the *Address Book* toolbar, activate the search option by clicking the **Find** field.

The field clears and a cursor appears indicating that the field is active.

3 Type all or part of the participant's name or group name and click the search button.



The closest matching participant entries are displayed and the Active Filter indicator turns on.

Filtering the Address Book

The entries in an address book group can be filtered to display only the entries (participants or groups) that meet criteria that you specify and hides entries that you do not want displayed. It enables you to select and work with a subset of *Address Book* entries.

You can filter by more than one column, by adding additional filters (columns).

The filter applies to the displayed group. If *All Participants* option is selected, it applies to all the listed participants.

Filtering can be done using:

- A predefined pattern
- Customized pattern

When you use the Find dialog box to search filtered data, only the data that is displayed is searched; data that is not displayed is not searched. To search all the data, clear all filters.

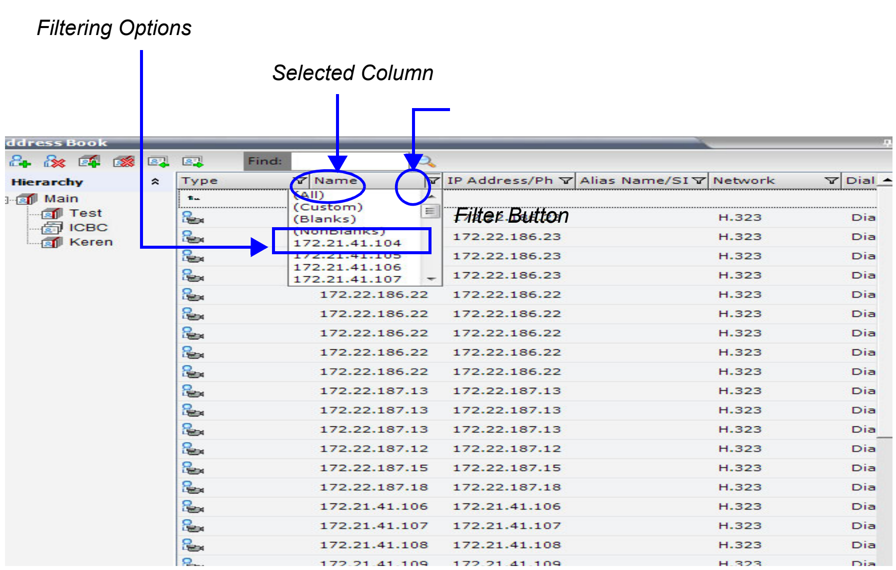
Filtering Address Book Data Using a Predefined Pattern

To filter the data in an address book group:

1 In the *Address Book - Navigation* pane, select the group to filter.

2 In the *Address Book - List* pane, in the *column* that you want to use for filtering, click the filter (▼) button.

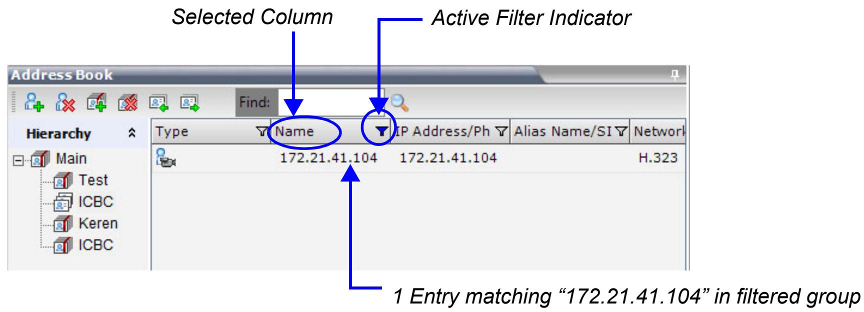
A drop-down menu is displayed containing all the matching patterns that can be applied to the selected field.



3 Click the matching pattern to be applied.

The filtered list is displayed with a filter indicator (▼) displayed in the selected column heading.

Example: If the user selects **172.21.41.104** as the matching pattern, the filtered group in the *Address Book* is displayed as follows:



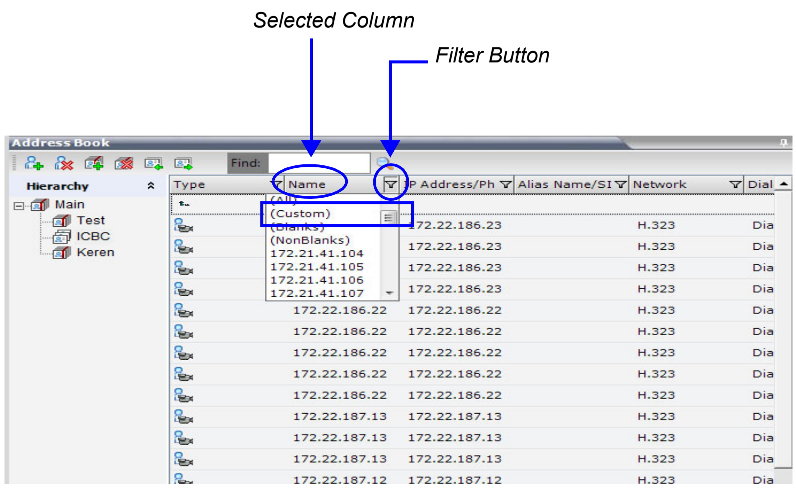
Filtering Address Book Data Using a Custom Pattern

To filter the data in an address book group:

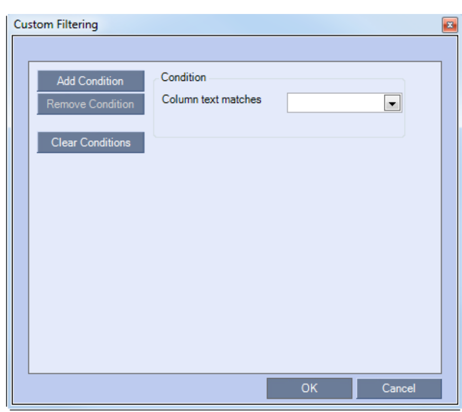
1 In the *Address Book - Navigation* pane, select the group to filter.

2 In the *Address Book - List* pane, in the *column* that you want to use for filtering, click the filter (▽) button.

3 Select the **(Custom)** option from the drop-down list.



The *Custom Filtering* dialog box opens.

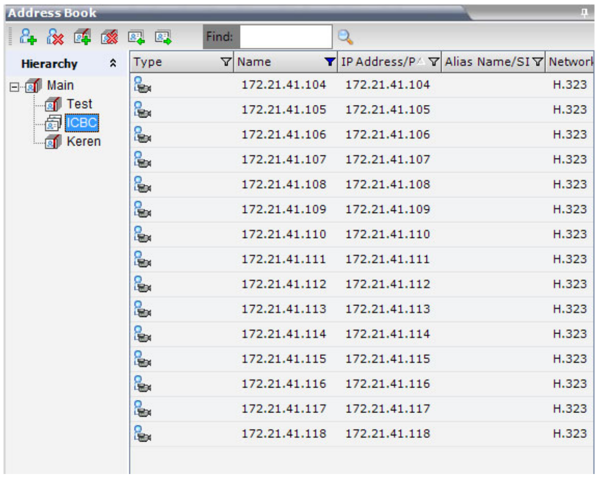


4 In the *Condition - Column text matches* field, enter the filtering pattern.
For example, to list only endpoints that include the numerals 41 in their name, enter 41.

5 **Optional.** Click the **Add Condition** button to define additional filtering patterns to further filter the list and fine tune your search.

To clear a filtering pattern, click the **Clear Condition** button.

The filtered list is displayed with an active filter (blue) indicator ( ) displayed in the selected column heading. For example, if the filtering pattern is 41, the participants list includes all the endpoints that contain the numerals 41 in their name.



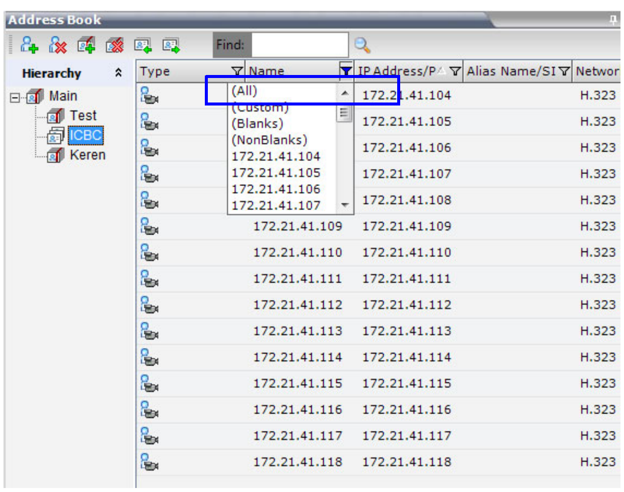
Clearing the Filter

To clear the filter and display all entries:

1 In the filtered *Address Book* column heading, click the *Active Filter* indicator.

The pattern matching options menu is displayed.

2 Click (**All)**.



The filter is deactivated and all the *group/level* entries are displayed.

Obtaining the Display Name from the Address Book

The MCU can be configured to replace the name of the dial-in participant as defined in the endpoint (site name) with the name defined in the Address Book.

In this process, the system retrieves the data (name, alias, number or IP address) of the dial-in participant and compares it first with the conference defined dial-in participants and if the endpoint is not found, it then searches for the endpoint with entries in the address book. After a match is found, the system displays the participant name as defined in the address book instead of the site name, in both the video layout and the RMX Web Client/Manager.

The system compares the following endpoint data with the address book entries:

- For H.323 participants, the system compares the IP address, Alias, or H.323 number.
- For SIP participants, the system compares the IP address or the SIP URI.

Guidelines

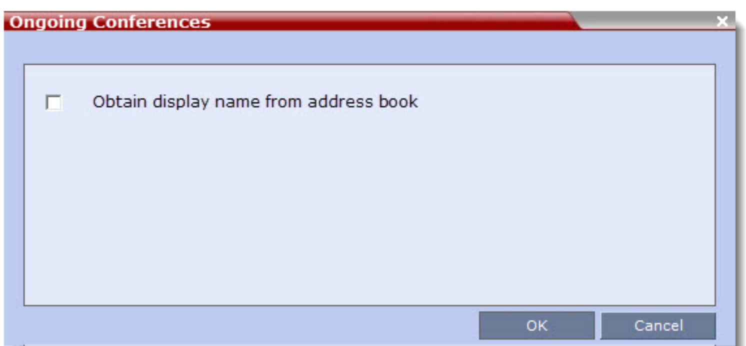
- Only Users with *Administrator* and *Operator* Authorization Levels are allowed to enable and disable the *Obtain Display Name from Address Book* feature.
- This feature is supported only for IPv4 participants.

Enabling and Disabling the Obtain Display Name from Address Book Feature

To enable or disable the Obtain Display Name from Address Book option:

1. On the RMX main menu bar, click **Setup > Customize Display Settings > Ongoing Conferences**.

   The *Ongoing Conferences* dialog box is displayed.

2. Select the **Obtain display name from address book** check box to enable the feature or clear the check box to disable the feature.
3. Click **OK**.

Importing and Exporting Address Books

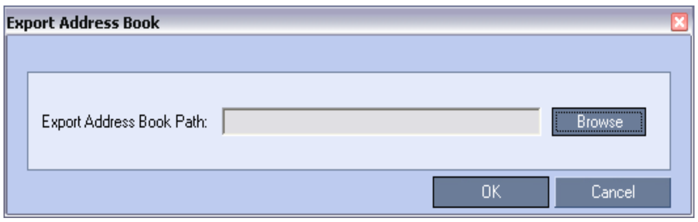
Address Books are proprietary Polycom data files that can only be distributed among RMX units. The Address Books are exported in XML format, which are editable offline. If no name is assigned to the exported Address Book, the default file name is:
`EMA.DataObjects.OfflineTemplates.AddressbookContent_.xml`

Exporting an Address Book

To Export an Address Book:

1 In the *Address Book* pane, click the **Export Address Book** ( ) button or right-click an empty area in the pane and click **Export Address Book**.

The *Export Address Book* dialog box is displayed.



2 Enter the desired path or click the **Browse** button.

3 In the **Save Address Book** dialog box, select the directory to save the file. You may also rename the file in the *File Name* field.

4 Click **Save**.

You will return to the *Export File* dialog box.

5 Click **OK**.

The exported Address Book is saved in the selected folder in XML format.

Importing an Address Book

To Import and Address Book:

1 In the *Address Book* pane, click the **Import Address Book** ( ) button or right-click an empty area in the pane and then click **Import Address Book**.

The *Import Address Book* dialog box is displayed.

2 Enter the path from which to import the Address Book or click the **Browse** button.

3 In the *Open* dialog box navigate to the desired Address Book file (in XML format) to import.

When importing an Address Book, participants with exact names in the current Address Book will be overwritten by participants defined in the imported Address Book.

4 Click **Open**.

You will return to the *Import File* dialog box.

5 Click **OK**.

The *Address Book* is imported and a confirmation message is displayed at the end of the process.

6 Click **Close**.

Upgrading and Downgrading Considerations

When upgrading to a multi-level address book version from a single-level address book, the following factors have to be taken into consideration:

- The system automatically creates a new address book with a different name and modifies the new address book to a multi-level hierarchical address book.
- By default, the address book contains two levels:
  - — The top level (root) named “Main”.
  - — Second level - All address book groups from the single-level address book are placed under the “Main” group with their associated participants.
- Participants that were not previously associated with any group in the Address Book are placed in the “Main” group.
- All participants in the Address Book appear in the “All Participants” group.
- During the upgrade process, the single-level address book file is save in the system to enable a future the downgrade of the version to a previous, single-level address book version (if required).

When downgrading from a multi-level address book version to a single-level address book version, the multi-level address book is replaced during the downgrade process by the single-level address book that was saved during the upgrade process.

Integrating the Polycom CMA™ Address Book with the RMX

The Polycom CMA™ application includes a Global Address Book with all registered endpoints. This address book can be used by the RMX 1500/2000/4000 to add participants to conferences.

CMA™ Address Book Integration Guidelines

- The RMX can use only one address book at a time. After you integrate the Polycom CMA with the Polycom RMX, the Polycom CMA address book replaces the RMX internal address book.

- The RMX uses the Polycom CMA address book in read-only mode. You can only add or modify CMA address book entries a from the CMA. Entries are also added when endpoints register with the CMA as gatekeeper.

The RMX acts as a proxy to all address book requests between the RMX Web Client and the CMA. **Ensure that firewall and other network settings allow the RMX access to the CMA server.**

To Integrate the Polycom CMA™ Address Book with the RMX:

CMA Side

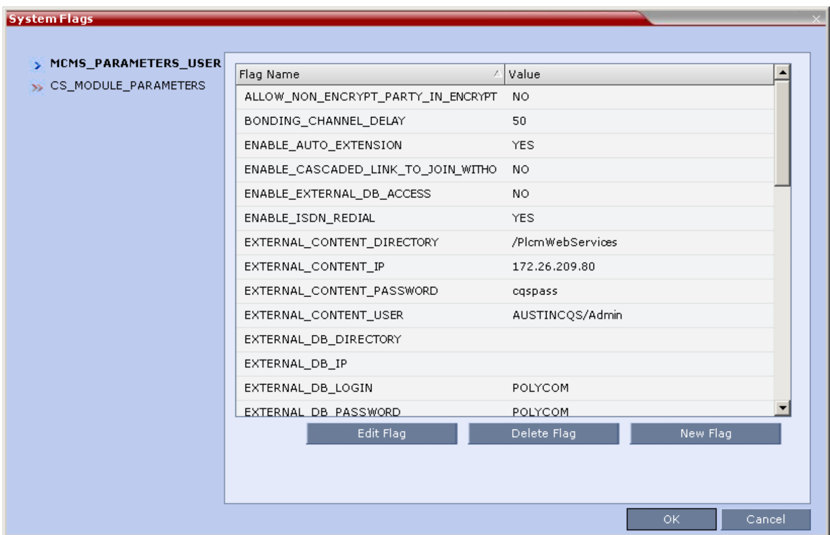
1 In the CMA application, manually add the Polycom RMX system to the Polycom CMA system as directed in the *Polycom CMA Operations Guide*.

2 In the CMA application, add a user or use an existing user for RMX login as directed in the *Polycom CMA Operations Guide*.
Write down the User Name and Password as they will be used later to define the RMX connection to the CMA Global Address Book.

RMX Side

1 On the *RMX* menu, click **Setup > System Configuration**.

The *System Flags - MCMS_PARAMETERS_USER* dialog box opens.



2 Modify the values of the following flags:

For more information, see "*Modifying System Flags*" on page **22-1**.

In versions 3.0 and earlier, these flags have to be manually added to the MCMS_PARAMETERS_USER dialog box. In version 4.0 and later, these flags are automatically listed in the MCMS_PARAMETERS_USER dialog box.

Table 8-7 *System Flags for CMA Address Book Integration*

Flag	Description
EXTERNAL_CONTENT_DIRECTORY	The Web Server folder name. Change this name if you have changed the default names used by the CMA application. Default: /PlcmWebServices

Table 8-7 System Flags for CMA Address Book Integration (Continued)

Flag	Description
EXTERNAL_CONTENT_IP	**Version 4.x and earlier -** enter the IP address of the CMA server. For example: 172.22.185.89. **Version 5.0.x and version 6.0.x** - enter the IP address of the CMA server in the format: **http://[IP address of the CMA server]**. For example, http://172.22.185.89. **Version 7.0.x and later -** enter the IP address of the CMA server. For example: 172.22.185.89. This flag is also the trigger for replacing the internal RMX address book with the CMA global Address Book. Leave this flag blank to disable address book integration with the CMA server.
EXTERNAL_CONTENT_PASSWORD	The password associated with the user name defined for the RMX in the CMA server.
EXTERNAL_CONTENT_USER	The login name defined for the RMX in the CMA server defined in the format: domain name/user name.

3 Click **OK** to complete the definitions.

4 When prompted, click **Yes** to reset the MCU and implement the changes to the system configuration.

9

Reservations

> Reservations are supported in AVC Conferencing Mode only.

The *Reservations* option enables users to schedule conferences. These conferences can be launched immediately or become ongoing, at a specified time on a specified date.

Scheduling a conference reservation requires definition of conference parameters such as the date and time at which the conference is to start, the participants and the duration of the conference.

Scheduled conferences (Reservations) can occur once or repeatedly, and the recurrence pattern can vary.

The maximum number of reservations per RMX are:

- **RealPresence Collaboration Server (RMX) 1500 -** 2000
- **RealPresence Collaboration Server (RMX) 2000 -** 2000
- **RealPresence Collaboration Server (RMX) 4000 -** 4000

Guidelines

System

- By default, the *Scheduler* is enabled by a *System Flag*. The flag prevents potential scheduling conflicts from occurring as a result of system calls from external scheduling applications such as *ReadiManager®, SE200 CMA™ 4000/5000* and others via the API.

  If an external scheduling application is used, the flag **INTERNAL_SCHEDULER** must be manually added to the *System Configuration* and its value must be set to NO.
  For more information see "*Modifying System Flags"* on page **22-1**.

Resources

- The maximum number of participants per reservation is determined by the availability of system resources:
  - RealPresence Collaboration Server (RMX) 1500 *MPMx-Q Mode*: 90 (25 video).
  - RealPresence Collaboration Server (RMX) 1500 *MPMx-S Mode*: 180 (45 video).
  - RealPresence Collaboration Server (RMX) 1500 *MPMx-D Mode*: 360 (90 video)
  - RealPresence Collaboration Server (RMX) 2000 *MPM Mode*: 400 (80 video).
  - RealPresence Collaboration Server (RMX) 2000 *MPM+ Mode*: 800 (160 video).
  - RealPresence Collaboration Server (RMX) 2000 *MPMx-D Mode*: 720 (180 video).
  - RealPresence Collaboration Server (RMX) 4000 *MPM+ Mode*: 1600 (160 video).

— RealPresence Collaboration Server (RMX) 4000 *MPMx-D Mode*: 1440 (180 video).

From *Version 7.1*, *MPM* media cards are not supported.

- System resources are calculated according to the RMX's license. For more information see "*Video/Voice Port Configuration"* on page **21-10**.
- System resource availability is partially checked when reservations are created:
  — If a conference duration extension request is received from an ongoing conference, the request is rejected if it would cause a resource conflict.
  — If several reservations are scheduled to be activated at the same time and there are not enough resources for all participants to be connected:
    - The conferences are activated.
    - Participants are connected to all the ongoing conferences until all system resources are used up.
- If sufficient resources are not available in the system and a scheduled *Reservation* cannot be activated, the *Reservation* is deleted from the schedule.
- Resources for *Reservations* are calculated using the *Reserve Resources for Audio/Video Participants* fields of the *New Reservation* dialog box. For more information see "*New Reservation – Reserved Resources"* on page **9-9**.
- Resources are reserved for participants at the highest video resolution supported by the *Line Rate* specified in the conference *Profile* and up to the maximum system video resolution specified by the *Resolution Configuration* dialog box.

  If the RMX is in *MPM+* or *MPMx Mode* and *Fixed Capacity Mode* is selected, the number of resources allocated to this type of video participant (CIF, SD, HD) is also checked. If resource deficiencies are found an error message is displayed.
- When a new *Reservation* is created in the *Reservation Calendar*, the effect of the new *Reservation* (including its recurrences) on available resources is checked. If resource deficiencies are found an error message is displayed.

  Defined dial-in or dial-out participants, Meeting Rooms, Entry Queues and new connections to Ongoing conferences are not included in the resources calculation.

Reservations

- A *Reservation* that has been activated and becomes an ongoing conference is deleted from the *Reservation Calendar* list.
- The maximum number of concurrent reservations is 80. Reservations with durations that overlap (for any amount of time) are considered to be concurrent.
- System resource availability is partially checked when reservations are created:
  — If a conference duration extension request is received from an ongoing conference, the request is rejected if it would cause a resource conflict.
  — If several reservations are scheduled to be activated at the same time and there are not enough resources for all participants to be connected:
    - The conferences are activated.
    - Participants are connected to all the ongoing conferences until all system resources are used up.
- A scheduled *Reservation* cannot be activated and is deleted from the schedule if an Ongoing conference has the same *Numeric ID*.

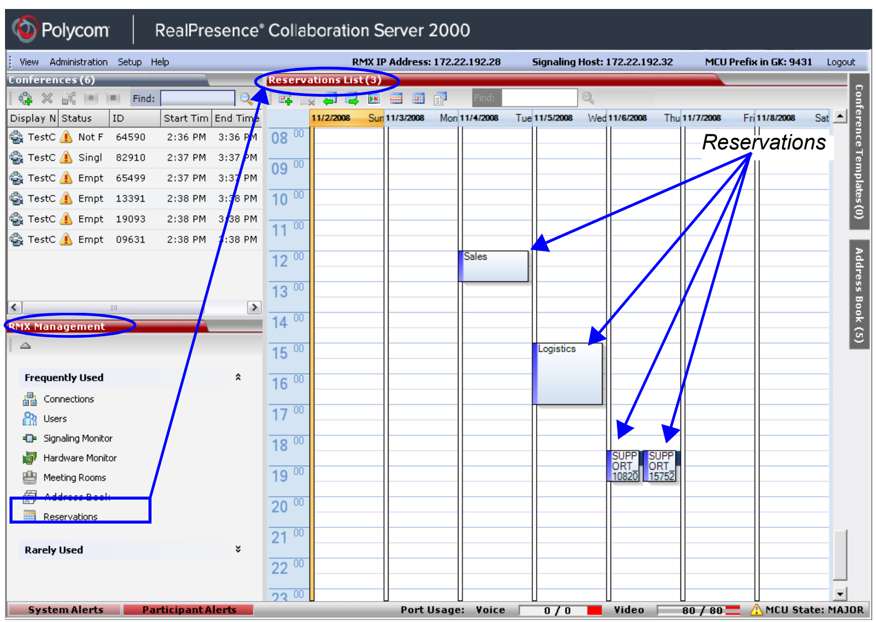
— Sufficient resources are not available in the system.

- If a problem prevents a *Reservation* from being activated at its schedule time, the *Reservation* will not be activated at all. This applies even if the problem is resolved during the *Reservation's* scheduled time slot.
- A Profile that is assigned to a Reservation cannot be deleted.
- Reservations are backed up and restored during **Setup > Software Management >Backup /Restore Configuration** operations. For more information see *"Banner Display and Customization"* on page **46**.
- All existing reservations are erased by the *Standard Restore* option of the **Administration > Tools > Restore Factory Defaults** procedure.
- *Reservations* can also be scheduled from *Conference Templates*. For more information see *"Scheduling a Reservation From a Conference Template (AVC Conferencing)"* on page **11**.

Using the Reservation Calendar

To open the Reservation Calendar:

>> In the *RMX Management* pane, click the *Reservation Calendar* button ( ).



Toolbar Buttons

The toolbar buttons functions are described in Table 9-1.

***Table 9-1** Reservations – Toolbar*

Button	Description
New Reservation	Create a new reservation. The date and time of the new reservation is set according to the highlighted blocks on the *Reservation Calendar*.
Delete Reservation	Click to delete the selected reservation.

***Table 9-1** Reservations – Toolbar (Continued)*

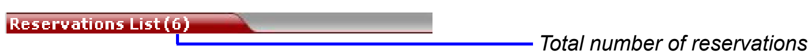
Button	Description
Back	Click to show the previous day or week, depending on whether *Show Day* or *Show Week* is the selected.
Next	Click to show the next day or week, depending on whether *Show Day* or *Show Week* is the selected.
Today	Click to show the current date in the Reservation Calendar in either *Show Day* or *Show Week* view.
Show Week	Change the calendar view to weekly display, showing a calendar week: Sunday through Saturday
Show Day	Click this button to show the day containing the selected time slot.
Reservations List	Click to change to List View and display a list of all reservations.
Find:	Used to search for reservations by *Display Name*. (Available in *Reservations List view* only).

Reservations Views

The *Reservation Calendar* list has the following views available:

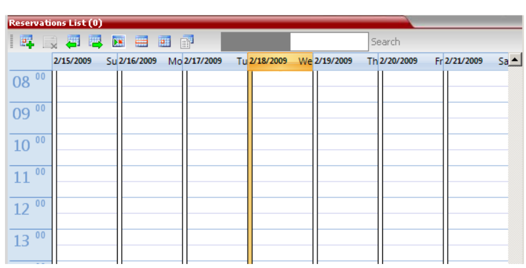
- Week
- Day
- Today
- List

In all views the *Main Window List Pane* header displays the total number of reservations in the system.



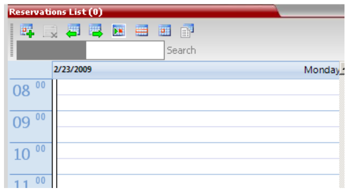
Week View

By default the *Reservation Calendar* is displayed in *Week* view with the current date highlighted in orange.



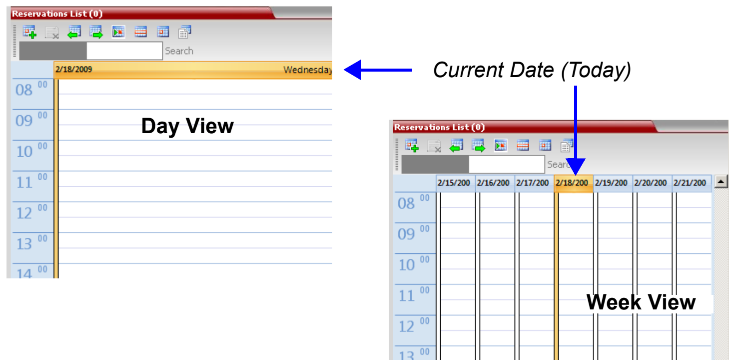
Day View

A single day is displayed.



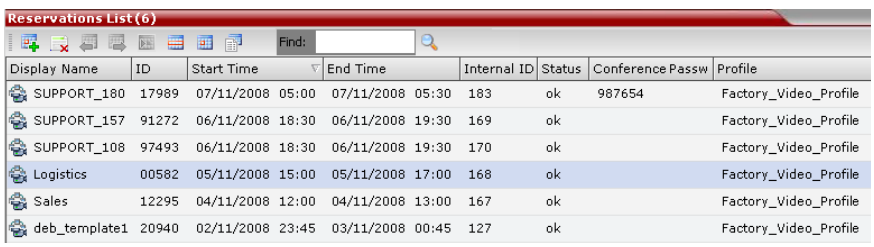
Today View

The current date (*Today*), highlighted in orange, can be viewed in both *Week View* and *Day View*.



List View

List View does not have a calendar based format.



Display Name	ID	Start Time	End Time	Internal ID	Status	Conference Passw	Profile
SUPPORT_180	17989	07/11/2008 05:00	07/11/2008 05:30	183	ok	987654	Factory_Video_Profile
SUPPORT_157	91272	06/11/2008 18:30	06/11/2008 19:30	169	ok		Factory_Video_Profile
SUPPORT_108	97493	06/11/2008 18:30	06/11/2008 19:30	170	ok		Factory_Video_Profile
Logistics	00582	05/11/2008 15:00	05/11/2008 17:00	168	ok		Factory_Video_Profile
Sales	12295	04/11/2008 12:00	04/11/2008 13:00	167	ok		Factory_Video_Profile
deb_template1	20940	02/11/2008 23:45	03/11/2008 00:45	127	ok		Factory_Video_Profile

All *Reservations* are listed by:

- *Display Name*
- *ID*
- *Internal ID*
- *Start Time*
- *End Time*
- *Status*
- *Conference Password*
- *Profile*

The *Reservations* can be sorted, searched and browsed by any of the listed fields.

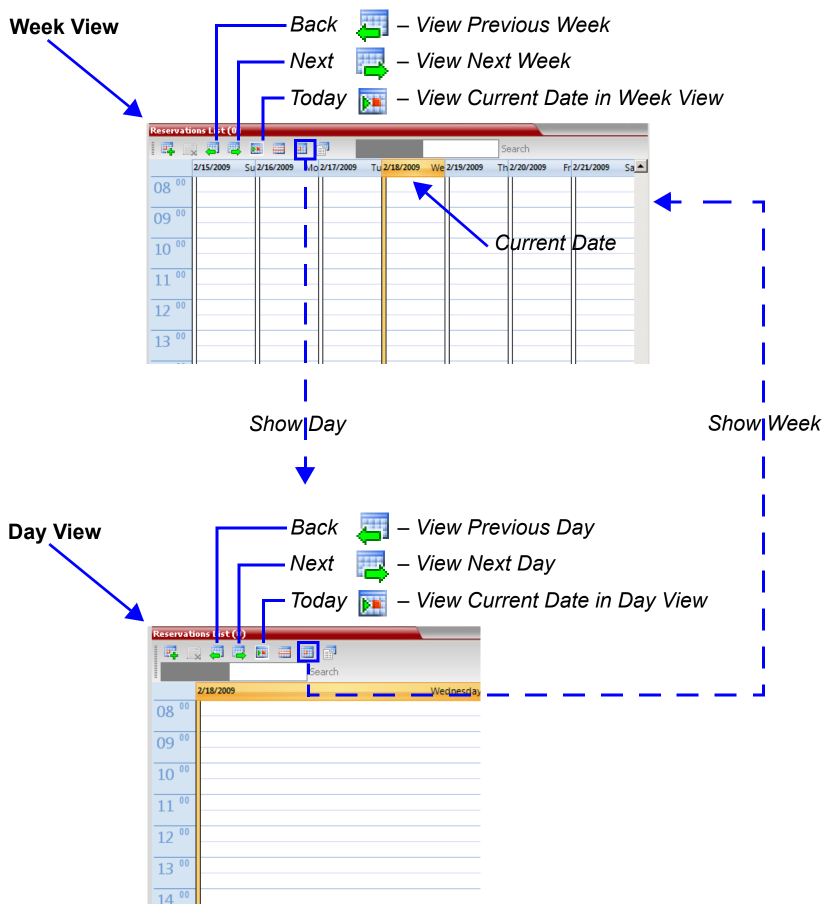
Changing the Calendar View

To change between Week and Day views:

>> In Week View: In the *Reservation Calendar* toolbar, click **Show Day** ( ) to change to *Day View*.

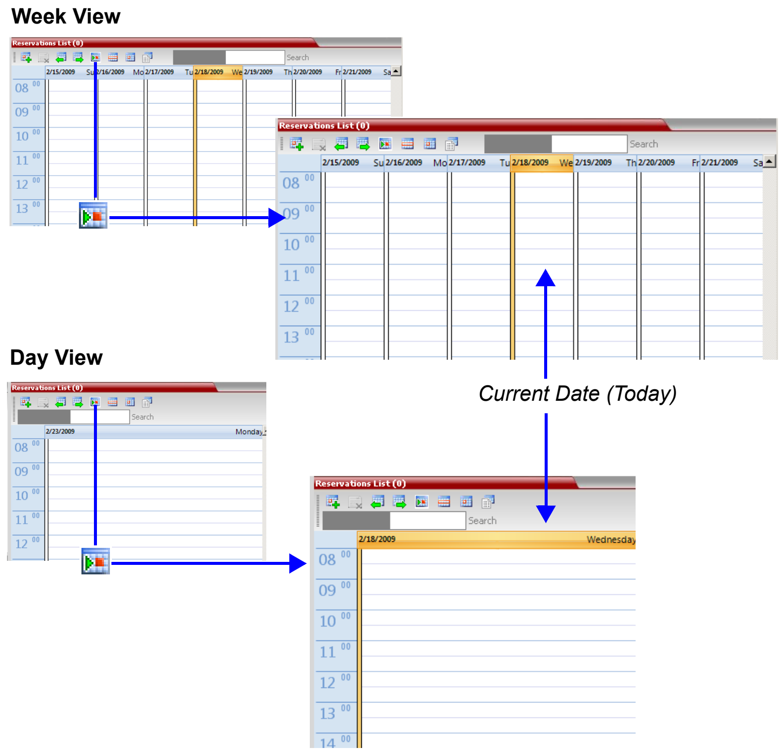
or

In Day View: In the *Reservation Calendar* toolbar, click **Show Week** ( ) to change to *Week View*.



To view Today (the current date):

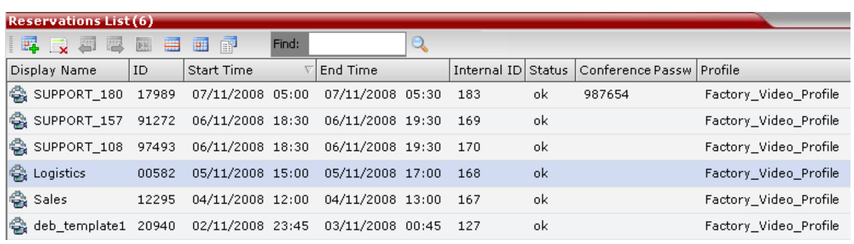
>> In *Week View* or *Day View*, in the *Reservation Calendar* toolbar, click the **Today** ( ) button to have the current date displayed within the selected view.



To change to List View:

1 In the *Reservation Calendar* toolbar, click, the **Reservations List** ( ) button.

The *Reservations List* is displayed.



Reservations List (6)

Display Name	ID	Start Time	End Time	Internal ID	Status	Conference Passw	Profile
SUPPORT_180	17989	07/11/2008 05:00	07/11/2008 05:30	183	ok	987654	Factory_Video_Profile
SUPPORT_157	91272	06/11/2008 18:30	06/11/2008 19:30	169	ok		Factory_Video_Profile
SUPPORT_108	97493	06/11/2008 18:30	06/11/2008 19:30	170	ok		Factory_Video_Profile
Logistics	00582	05/11/2008 15:00	05/11/2008 17:00	168	ok		Factory_Video_Profile
Sales	12295	04/11/2008 12:00	04/11/2008 13:00	167	ok		Factory_Video_Profile
deb_template1	20940	02/11/2008 23:45	03/11/2008 00:45	127	ok		Factory_Video_Profile

2 **Optional.** Sort the data by any field (column heading) by clicking on the column heading.

A ▽ or △ symbol is displayed in the column heading indicating that the list is sorted by this field, as well as the sort order.

3 **Optional.** Click on the column heading to toggle the column's sort order.

To return to Calendar View:

>> In the *Reservation Calendar* toolbar, click any of the buttons (**Show Week**/**Show Day**/ **Today**) to return to the required *Reservation Calendar* view.

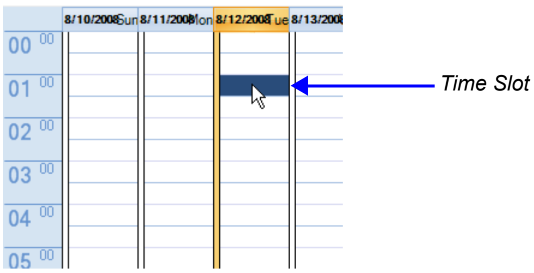
Scheduling Conferences Using the Reservation Calendar

Creating a New Reservation

There are three methods of creating a new reservation:

Each method requires the selection of a starting time slot in the *Reservation Calendar*. The default time slot is the current half-hour period of local time.

In all views, if the **New Reservation** ( ) button is clicked without selecting a starting time slot or if a time slot is selected that is in the past, the *Reservation* becomes an Ongoing conference immediately and is not added to the *Reservations* calendar.



After selecting a starting time slot in the *Reservation Calendar* you can create a reservation with a default duration derived from the creation method used or by interactively defining the duration of the reservation.

Method I – To create a reservation with default duration of 1 hour:

>> In the *Reservation Calendar* toolbar, click the **New Reservation** ( ) button to create a reservation of 1 hour duration.

Method II – To create a reservation with default duration of ½ hour:

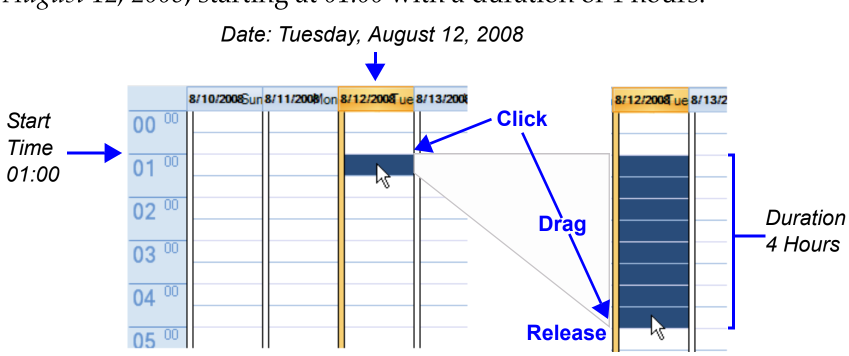
>> Right-click and select **New Reservation** to create a reservation of ½ hour default duration.

Method III – To interactively define the duration:

1 In the calendar, click & drag to expand the time slot to select the required *Date*, *Start Time and Duration* for the reservation.

2 In the *Reservation Calendar* toolbar, click the **New Reservation** ( ) button or right-click and select **New Reservation.**

Example: The following click & drag sequence would select a reservation for *Tuesday, August 12, 2008*, starting at *01:00* with a duration of *4* hours.



The duration of reservations created by any of the above methods can be modified in the *Scheduler* tab of the *New Reservation* dialog box.

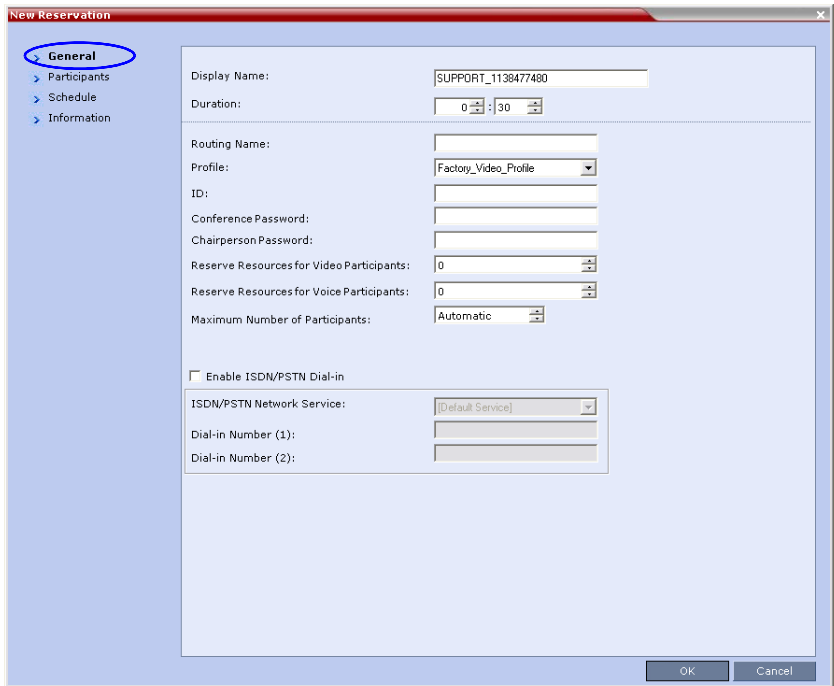
To create a new reservation:

1 Open the *Reservation Calendar*.

2 Select a starting time slot.

3 Create the reservation using one of the three methods described above.

The *New Reservation – General* tab dialog box opens.



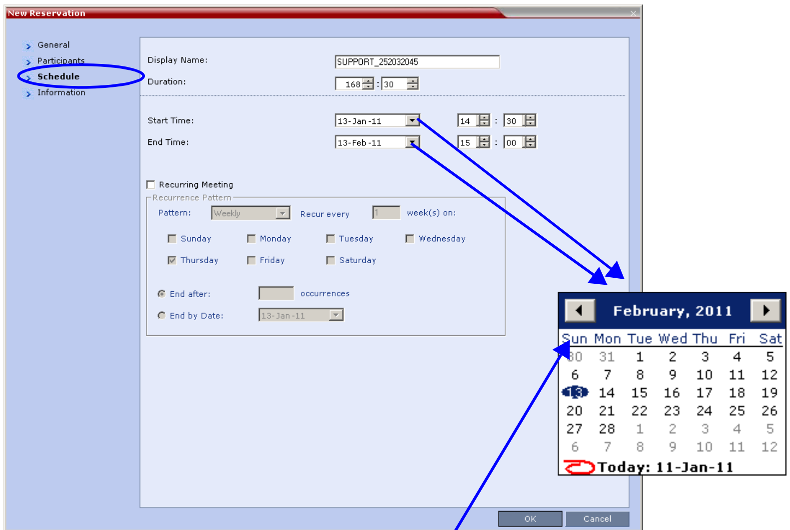
All the fields are the same as for the *New Conference – General* tab, described in the RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "*General Tab"* on page **3-14**.

Table 9-2 *New Reservation – Reserved Resources*

Field	Description
Reserve Resources for Video Participants	Enter the number of video participants for which the system must reserve resources. Default: 0 participants.
Reserve Resources for Audio Participants	Enter the number of audio participants for which the system must reserve resources. Default: 0 participants.

> When a Conference Profile is assigned to a Meeting Room or a Reservation, the Profile’s parameters are not embedded in the Reservation, and are taken from the Profile when the reservation becomes an ongoing conference. Therefore, any changes to the Profile parameters between the time the Reservation or Meeting Room was created and the time that it is activated (and becomes an ongoing conference) will be applied to the conference.
> If the user wants to save the current parameters, a different Profile with these parameters must be assigned, or a different Profile with the new parameters must be created.

4 Click the **Schedule** tab.



Calendar

5 Adjust the new reservation's schedule by modifying the fields as described in Table 9-3.

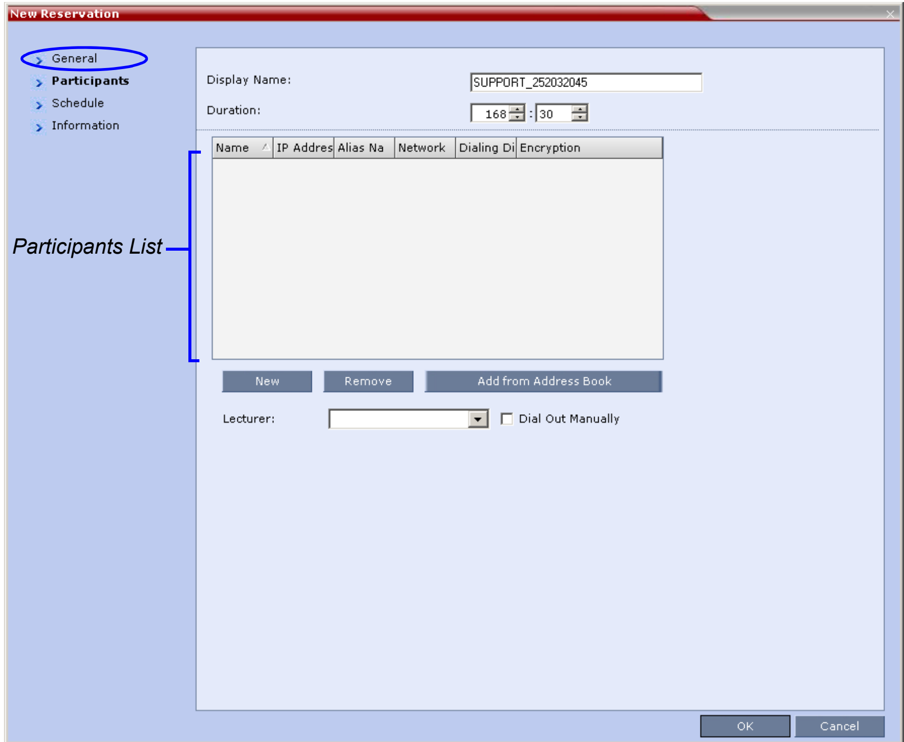
Table 9-3 *New Reservation – Schedule Tab*

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>Start Time</td><td>Select the Start Time of the Reservation.</td><td rowspan="2">The Start/End Times of the Reservation are initially taken from the time slot selected in the Reservation Calendar.
The Start/End Times can be adjusted by typing in the hours and minutes fields or by clicking the arrow buttons.
The Start/End dates can be adjusted by typing in the date field or by clicking the arrow buttons or using the calendar.
The start time of all the reservations can be manually adjusted in one operation. For more information see "Adjusting the Start Times of all Reservations” on page 9-16.
End Time settings are initially calculated as Start Time + Duration. End Time settings are recalculated if Start Time settings are changed.
Changes to End Time settings do not affect Start Time settings. However, the Duration of the Reservation is recalculated.</td></tr>
<tr><td>End Time</td><td>Select the End Time of the Reservation.</td></tr>
<tr><td>Recurring Meeting</td><td colspan="2">Select this option to set up a Recurring Reservation - a series of Reservations to be repeated on a regular basis.
To create a recurring reservation, you must define a time period and a recurrence pattern of how often the Reservation should occur: Daily, Weekly or Monthly.</td></tr>
</table>

Table 9-3 *New Reservation – Schedule Tab (Continued)*

Field	Description	
Recurrence Pattern	Daily	If *Daily* is selected, the system automatically selects all the days of the week. To de-select days (for example, weekends) clear their check boxes.
	Weekly	If *Weekly* is selected, the system automatically selects the day of the week for the Reservation from the day selected in the Reservation Calendar. You can also define the recurrence interval in weeks. For example, if you want the reservation to occur every second week, enter 2 in the *Recur every _ week(s)* field. To define a twice-weekly recurring Reservation, select the check box of the additional day of the week on which the Reservation is to be scheduled and set the recurrence interval to 1.
	Monthly	If *Monthly* is selected, the system automatically selects the day of the month as selected in the Reservation Calendar. You are required to choose a recurrence pattern: • **Day (1-31) of every (1-12) month(s**) - Repeats a conference on a specified day of the month at a specified monthly interval. For example, if the first Reservation is scheduled for the 6th day of the current month and the monthly interval is set to 1, the monthly Reservation will occur on the 6th day of each of the following months. • **The (first, second,...,last) (Sun-Sat) of x month(s)** - Repeats a Reservation in a particular week, on a specified day of the week at the specified monthly interval. For example, a recurrent meeting on the third Monday every second month.
A series of Reservations can be set to end after a specified number of occurrences or by a specific date. Select one of the following methods of terminating the series of Reservations:		
End After	**End After: x Occurrences** - Ends a recurring series of Reservations after a specific number (x) of occurrences. Default: 1 (Leaving the field blank defaults to 1 occurrence.)	
End by Date	**End By Date: mm/dd/yyyy** - Specifies a date for the last occurrence of the recurring series of Reservations. The End By Date value can be adjusted by typing in the date field or by clicking the arrow button and using the calendar utility. Default: Current date.	

6 Click the **Participants** tab.



The fields are the same as for the *New Conference – Participants* tab, described in the RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "*Participants Tab"* on page **3-17**.

Participant properties are embedded in the conferencing entity and therefore, if the participant properties are modified in the *Address Book* (or *Meeting Rooms*) after the Reservation has been created they are not applied to the participant when the Reservation is activated.

7 **Optional.** Add participants from the *Participants Address Book*.

For more information see "*Meeting Rooms"* on page **6-1** and the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guidee*, "*To add participants from the Address Book:"* on page **3-19**.

8 **Optional.** Add information to the reservation.

Information entered in the *Information* tab is written to the *Call Detail Record (CDR)* when the reservation is activated. Changes made to this information before it becomes an ongoing conference will be saved to the CDR.

For more information see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "*Information Tab"* on page **3-20**.

9 Click **OK**.
The *New Reservation* is created and is displayed in the *Reservation Calendar*.

If you create a recurring reservation all occurrences have the same ID. A recurring Reservation is assigned the same ISDN/PSTN dial-in number for all recurrences.

If a dial in number conflict occurs prior to the conference's start time, an alert is displayed: "ISDN dial-in number is already assigned to another conferencing entity" and the conference cannot start.

The series number (_0000n) of each reservation is appended to its *Display Name*.

Example:

Conference Template name: Sales

Display Name for single scheduled occurrence: Sales

If 3 recurrences of the reservation are created:

Display Name for occurrence 1: Sales**_00001**

Display Name for occurrence 2: Sales_**00002**

Display Name for occurrence 3: Sales_**00003**

Managing Reservations

Reservations can be accessed and managed via all the views of the *Reservations List*.

Guidelines

- The *Recurrence Pattern* fields in the *Schedule* tab that are used to create multiple occurrences of a *Reservation* are only displayed when the *Reservation* and its multiple occurrences are initially created.
- As with single occurrence *Reservations*, only the *Duration*, *Start Time* and *End Time* parameters of multiple occurrence reservations can be modified after the *Reservation* has been created.
- A single occurrence *Reservation* cannot be modified to become a multiple occurrence reservation.
- *Reservations* can only be modified one at a time and not as a group.
- If *Reservations* were created as a recurring series, the system gives the option to delete them individually, or all as series.

Viewing and Modifying Reservations

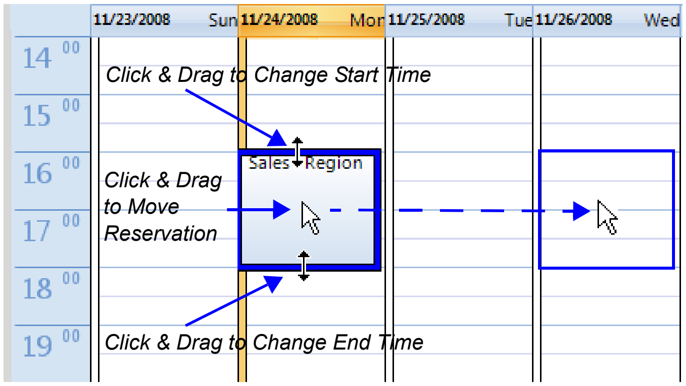
Reservations can be viewed and modified by using the *Week* and *Day* views of the *Reservations Calendar* or by using the *Reservation Properties* dialog box.

Using the Week and Day views of the Reservations Calendar

In the *Week* and *Day* views each *Reservation* is represented by a shaded square on the *Reservation Calendar*. Clicking on a *Reservation* selects the *Reservation*. A dark blue border is displayed around the edges of the *Reservation* indicating that it has been selected.

The *Start Time* of the *Reservation* is represented by the top edge of the square while the *End Time* is represented by the bottom edge.

The cursor changes to a vertical double arrow (↕) when it is moved over the top and bottom sides of the square.



To move the Reservation to another time slot:

1 Select the *Reservation*.

2 Hold the mouse button down and drag the *Reservation* to the desired time slot.

3 Release the mouse button.

To change the Reservation's Start time:

1 Select the *Reservation*.

2 Move the mouse over the top edge of the *Reservation's* square.

3 When the cursor changes to a vertical double arrow (↕) hold the mouse button down and drag the edge to the desired *Start Time*.

4 Release the mouse button.

To change the Reservation's End time:

1 Select the *Reservation*.

2 Move the mouse over the bottom edge of the *Reservation's* square.

3 When the cursor changes to a vertical double arrow (↕) hold the mouse button down and drag the edge to the desired *End Time*.

4 Release the mouse button.

To View or Modify Reservations using the Reservation Properties dialog box:

1 In the *Reservations List*, navigate to the reservation (or its recurrences) you want to view, using the **Show Day**, **Show Week**, **Today**, **Back**, **Next** or **List** buttons.

2 Double-click, or right-click and select **Reservation Properties**, to select the reservation to be viewed or modified.

   The *Reservation Properties – General* dialog box opens.

3 Select the tab(s) of the properties you want to view or modify.

4 **Optional.** Modify the *Reservation Properties*.

5 Click **OK**.
   The dialog box closes and modifications (if any) are saved.

Adjusting the Start Times of all Reservations

When utilizing GMT offset (for example, *Daylight Saving Time* change), the start time of the reoccurring reservations scheduled before the RMX time change are not updated accordingly (although their start times appear correctly in the *Reservations* list, when checking the reservation properties the start time is incorrect).

Following the RMX time change, the start time of all reoccurring reservations must be manually adjusted in one operation.

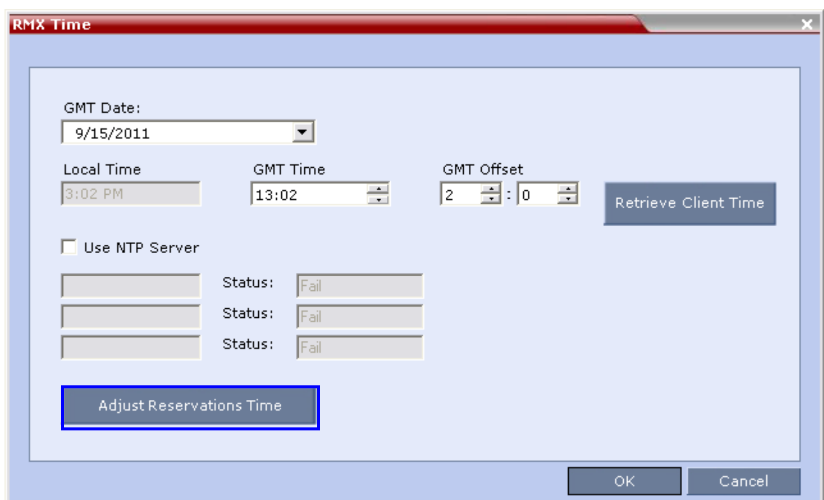
Using this option, the start times of **all** reservations currently scheduled on the RMX are adjusted with the same offset.

To adjust the reoccurring reservations start time after the GMT Offset has been changed for Daylight Saving Time (DST) or a physical move:.

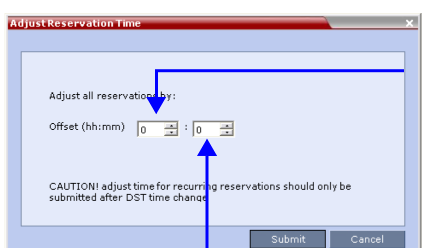
> Adjustment of *Reservation Time* should only be performed after adjustment of *RMX Time* is completed as a separate procedure.

1 On the RMX menu, click **Setup > RMX Time**.
The *RMX Time* dialog box opens.

2 Click the **Adjust Reservations Time** button.



The *Adjust Reservations Time* dialog box opens.



Click the arrows to adjust the start time by hours.
Range is between 12 hours and -12 hours
A positive value indicates adding to the start time
(-) indicates subtracting from the start time

Click the arrows to adjust the start time by minutes.
Range is between 45 minutes and -45 minutes.
A positive value indicates adding to the start time
(-) indicates subtracting from the start time

3 Click the arrows of the *Offset - Hours* box to indicate the number of hours to add or subtract from the current start time; a positive value indicates adding time, while minus (-) indicates subtracting time.

4 Click the arrows of the *Offset - minutes* box to indicate the number of minutes to add or subtract from the current start time of the reservations. Increments or decrements are by 15 minutes.

For example, to subtract 30 minutes from the start time of all the reservation, enter 0 in the *hours* box, and -30 in the *minutes* box.

To add one hour and 30 minutes to the start time, enter 1 in the hours box and 30 in the minutes box.

5 Click the **Adjust** button to apply the change to all the reoccurring reservations currently scheduled on the RMX.

> When adjusting the start time of 1000 - 2000 reservations, an “Internal communication error” message may appear. Ignore this message as the process completes successfully.

Deleting Reservations

To delete a single reservation:

1 In the *Reservations List*, navigate to the reservation you want to delete, using the **Show Day**, **Show Week**, **Today**, **Back**, **Next** or **List** buttons.

2 Click to select the reservation to be deleted.

3 Click the **Delete Reservation** ( ) button.
or
Place the mouse pointer within the *Reservation* block, right-click and select **Delete Reservation**.

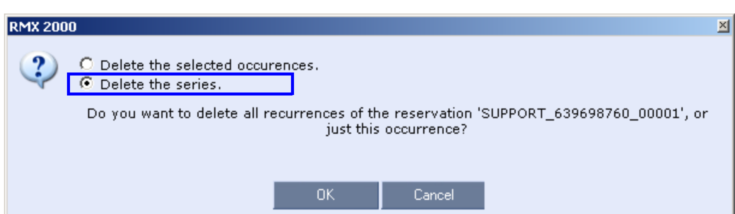
4 Click **OK** in the confirmation dialog box.
The *Reservation* is deleted.

To delete all recurrences of a reservation:

1 In the *Reservations List*, navigate to the *Reservation* or any of its recurrences, using the **Show Day**, **Show Week**, **Today**, **Back**, **Next** or **List** buttons.

2 Click the **Delete Reservation** ( ) button.
or
Place the mouse pointer within the *Reservation* or any of its recurrences, right-click and select **Delete Reservation**.

A confirmation dialog box is displayed.



3 Select **Delete the series.**

4 Click **OK.**

All occurrences of the *Reservation* are deleted.

Searching for Reservations using Quick Search

Quick Search is available only in *List View*. It enables you to search for *Reservations* by *Display Name*.

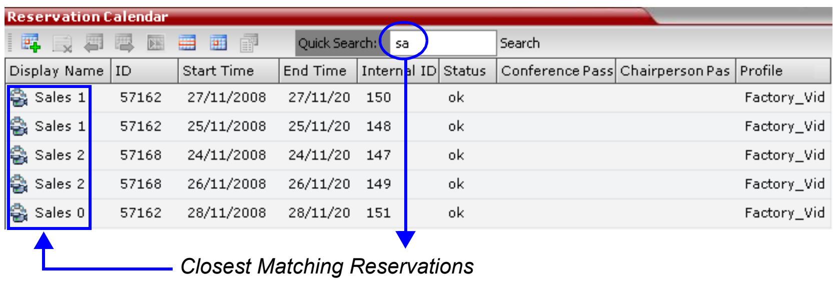
To search for reservations:

1 In the *Reservation Calendar* toolbar, click in the *Quick Search* field.

The field clears and a cursor is displayed indicating that the field is active.

2 Type all or part of the reservation's *Display Name* into the field and click **Search**.

The closest matching *Reservation* entries are displayed.



3 **Optional.** Double- click the *Reservation's* entry in the list to open the *Reservations Properties* dialog box to view or modify the *Reservation*.

or

Right -click the *Reservation's* entry in the list and select a menu option to view, modify or delete the *Reservation*.

To clear the search and display all reservations:

1 Clear the *Quick Search* field.

2 Click **Search.**

All *Reservations* are displayed.

10

Operator Assistance & Participant Move

> Operator conferences and participant move are supported in AVC Conferencing Mode only.

Users (operators) assistance to participants is available when:

- Participants have requested individual help (using *0 DTMF code) during the conference.
- Participants have requested help for the conference (using 00 DTMF code) during the conference.
- Participants have problems connecting to conferences, for example, when they enter the wrong conference ID or password.

In addition, the user (operator) can join the ongoing conference and assist all conference participants.

Operator assistance is available only when an *Operator conference* is running on the MCU.

The *Operator conference* offers additional conference management capabilities to the RMX users, enabling them to attend to participants with special requirements and acquire participant details for billing and statistics. This service is designed usually for large conferences that require the personal touch.

Operator assistance is available in MPM, MPM+ and MPMx *Card Configuration Modes*.

> From *Version 7.1*, *MPM* media cards are not supported.

Operator Conferences

An *Operator conference* is a special conference that enables the RMX user acting as an operator to assist participants without disturbing the ongoing conferences and without being heard by other conference participants. The operator can move a participant from the Entry Queue or ongoing conference to a private, one-on-one conversation in the Operator conference.

In attended mode, the RMX user (operator) can perform one of the following actions:

- Participants connected to the Entry Queue who fail to enter the correct destination ID or conference password can be moved by the user to the Operator conference for assistance.
- After a short conversation, the operator can move the participant from the Operator conference to the appropriate destination conference (Home conference).

- The operator can connect participants belonging to the same destination conference to their conference simultaneously by selecting the appropriate participants and moving them to the Home conference (interactively or using the right-click menu).
- The operator can move one or several participants from an ongoing conference to the *Operator conference* for a private conversation.
- The operator can move participants between ongoing Continuous Presence conferences.

Operator Conference Guidelines

- An *Operator conference* can only run in Continuous Presence mode.
- *Operator conference* is defined in the Conference Profile. When enabled in Conference Profile, *High Definition Video Switching* option is disabled.
- An *Operator conference* can only be created by a User with Operator or Administrator *Authorization* level.
- *Operator conference* name is derived from the User Login Name and it cannot be modified.
- Only one *Operator conference* per User *Login Name* can be created.
- When created, the *Operator conference* must include one and only one participant - the Operator participant.
- Only a defined dial-out participant can be added to an *Operator conference* as an Operator participant
- Once running, the RMX user can add new participants or move participants from other conferences to this conference. The maximum number of participants in an *Operator conference* is the same as in standard conferences.
- Special icons are used to indicate an *Operator conference* in the Ongoing Conferences list and the operator participant in the Participants list.
- An *Operator conference* cannot be defined as a Reservation.
- An *Operator conference* can be saved to a Conference Template. An ongoing *Operator conference* can be started from a Conference Template.
- The Operator participant cannot be deleted from the *Operator conference* or from any other conference to which she/he was moved to, but it can be disconnected from the conference.
- When deleting or terminating the *Operator conference*, the operator participant is automatically disconnected from the MCU, even if participating in a conference other than the *Operator conference*.
- Participants in Telepresence conferences cannot be moved from their conference, but an operator can join their conference and help them if assistance is required.
- Moving participants from/to an *Operator conference* follows the same guidelines as moving participants between conferences. For move guidelines, see "*Move Guidelines"* on page **10-18**.
- When a participant is moved from the Entry Queue to the *Operator conference*, the option to move back to the source (Home) conference is disabled as the Entry Queue is not considered as a source conference.
- The conference chairperson cannot be moved to the *Operator conference* following the individual help request if the *Auto Terminate When Chairperson Exits* option is enabled, to prevent the conference from automatically ending prematurely. In such a case, the assistance request is treated by the system as a conference assistance request, and the operator can join the conference.

Defining the Components Enabling Operator Assistance

To enable operator assistance for conferences, the following conferencing entities must be adjusted or created:

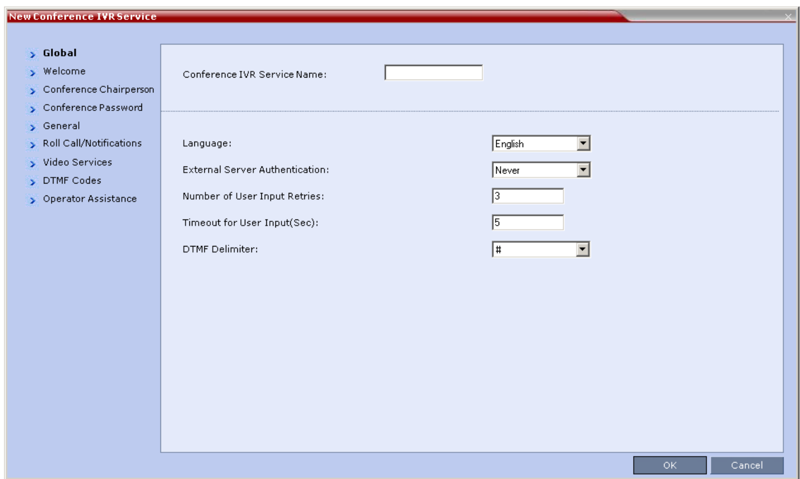
- IVR Service (Entry Queue and Conference) in which Operator Assistance options are enabled.
- A Conference Profile with the *Operator Conference* option enabled.
- An active Operator conference with a connected Operator participant.

Defining a Conference IVR Service with Operator Assistance Options

In the *RMX Management* pane, expand the *Rarely Used* list and click the **IVR Services** ( ) entry.

1 On the *IVR Services* toolbar, click the **New Conference IVR Service** (*) button.*

The *New Conference IVR Service - Global* dialog box opens.



2 Enter the *Conference IVR Service Name*.

3 Define the *Conference IVR Service - Global* parameters. For more information, see *Table 17-3, "Conference IVR Service Properties - Global Parameters,"* on page **17-7**.

4 Click the **Welcome** tab.
The *New Conference IVR Service - Welcome* dialog box opens.

5 Define the system behavior when the participant enters the Conference IVR queue. For more information, see "*Defining a New Conference IVR Service"* on page **17-6**.

6 Click the **Conference Chairperson** tab.
The *New Conference IVR Service - Conference Chairperson* dialog box opens.

7 If required, enable the chairperson functionality and select the various voice messages and options for the chairperson connection. For more information, see *Table 17-4, "New Conference IVR Service Properties - Conference Chairperson Options and Messages,"* on page **17-9**.

8 Click the **Conference Password** tab.

The *New Conference IVR Service - Conference Password* dialog box opens.

9 If required, enable the request for conference password before moving the participant from the conference IVR queue to the conference and set the MCU behavior for password request for *Dial-in* and *Dial-out* participant connections. For more information, see *Table 17-5, "New Conference IVR Service Properties - Conference Password Parameters,"* on page **17-10**.

10 Select the various audio messages that will be played in each case. For more information, see *Table 17-5, "New Conference IVR Service Properties - Conference Password Parameters,"* on page **17-10**.

11 Click the **General** tab.
The *New Conference IVR Service - General* dialog box opens.

12 Select the messages that will be played during the conference. For more information, see *Table 17-6, "Conference IVR Service Properties - General Voice Messages,"* on page **17-11**.

13 Click the **Roll Call/Notifications** tab.
The *New Conference IVR Service - Roll Call* dialog box opens.

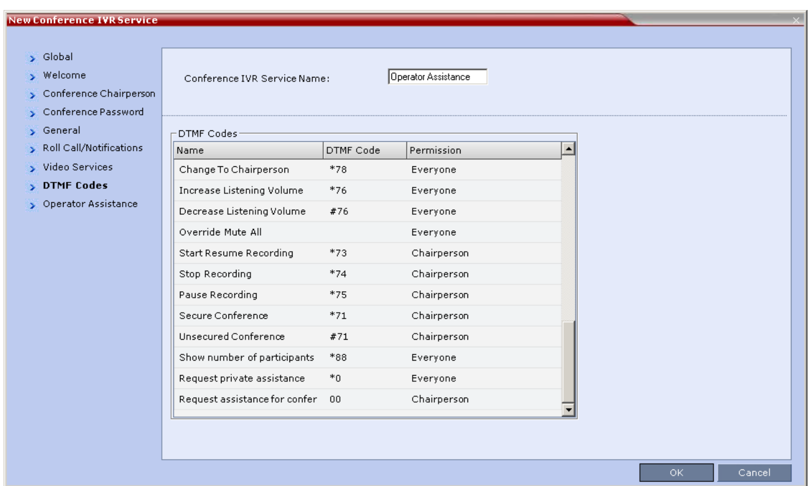
14 Enable the Roll Call feature and assign the appropriate audio file to each message type. For more information, see *Table 17-7, "Conference IVR Service Properties - Roll Call Messages,"* on page **17-14**.

15 Click the **Video Services** tab.
The *New Conference IVR Service - Video Services* dialog box opens.

16 Define the *Video Services* parameters. For more information, see *Table 17-9, "New Conference IVR Service Properties - Video Services Parameters,"* on page **17-17**.

17 Click the **DTMF Codes** tab.

The *New Conference IVR Service - DTMF Codes* dialog box opens.



The default DTMF codes for the various functions that can be performed during the conference by all participants or by the chairperson are listed. For the full list of the available DTMF codes, see *Table 17-10, "New Conference IVR Service Properties - DTMF Codes,"* on page **17-19**.

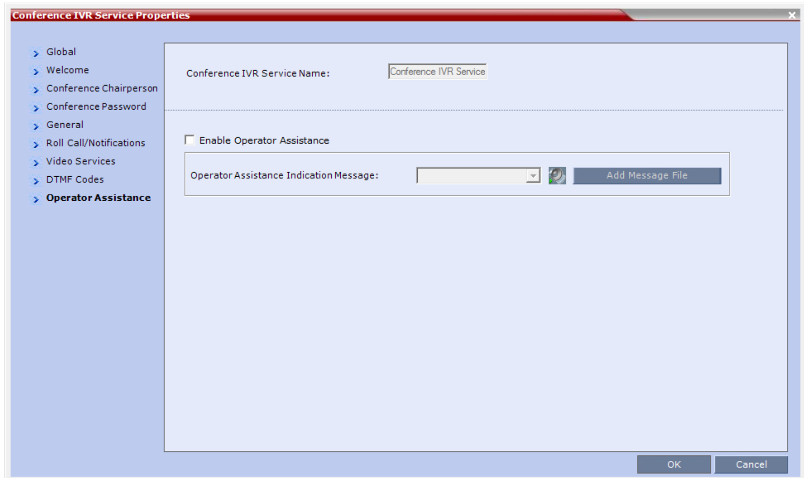
18 If required, modify the default DTMF codes and the permissions for various operations including Operator Assistance options:

— ***0** for individual help - the participant requested help for himself or herself. In such a case, the participant requesting help is moved to the Operator conference for one-on-one conversation. By default, all participants can use this code.

— **00** for conference help - the conference chairperson (default) can request help for the conference. In such a case, the operator joins the conference.

19 Click the **Operator Assistance** tab.

The *Operator Assistance* dialog box opens.



20 Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process to the conference or during the conference.

21 In the *Operator Assistance Indication Message* field, select the audio message to be played when the participant requests or is waiting for the operator's assistance.

> If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the RMX.

22 Click **OK** to complete the IVR Service definition.
The new Conference IVR Service is added to the *IVR Services* list.

Defining an Entry Queue IVR Service with Operator Assistance Options

1 In the *RMX Management* pane, click **IVR Services** ( ).

2 In the *IVR Services* list, click the **New Entry Queue IVR Service** ( ) button.

The *New Entry Queue IVR Service - Global* dialog box opens.

3 Define the *Entry Queue Service Name*.

4 Define the Entry Queue IVR Service Global parameters. For more information, see Table 17-11, "*Entry Queue IVR Service Properties - Global Parameters,*" on page 17-22.

5 Click the **Welcome** tab.
The *New Entry Queue IVR Service - Welcome* dialog box opens.

6 Define the system behavior when the participant enters the Entry Queue. This dialog box contains options that are identical to those in the *Conference IVR Service - Welcome Message* dialog box. For more information, see *"Welcome tab" on page* 13-11.

7 Click the **Conference ID** tab.
The *New Entry Queue IVR Service - Conference ID* dialog box opens.

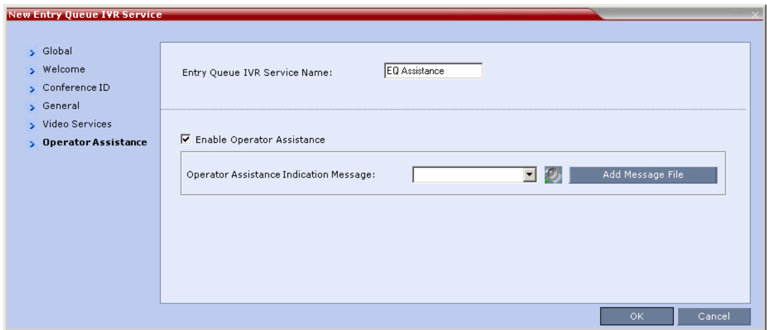
8 Select the required voice messages. For more information, see *Table 17-12, "Entry Queue IVR Service Properties - Conference ID,"* on page 17-23.

9 Click the **Video Services** tab.
The *New Entry Queue IVR Service - Video Services* dialog box opens.

10 In the *Video Welcome Slide* list, select the video slide that will be displayed to participants connecting to the Entry Queue. The slide list includes the video slides that were previously uploaded to the MCU memory.

11 Click the **Operator Assistance** tab.

The *Operator Assistance* dialog box opens.



12 Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process.

13 In the *Operator Assistance Indication Message* field, select the audio message to be played when the participant requests or is waiting for operator's assistance.

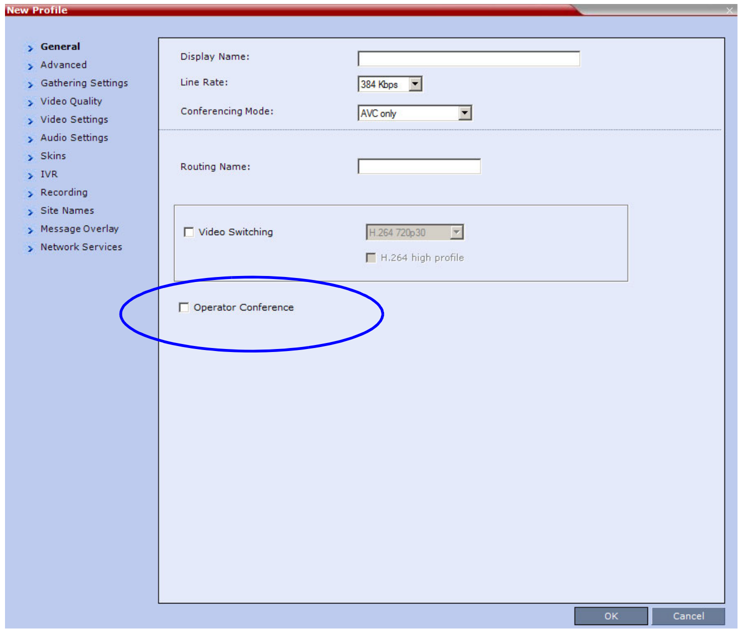
If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the RMX.

14 Click **OK** to complete the Entry Queue IVR Service definition.
The new Entry Queue IVR Service is added to the *IVR Services* list.

Defining a Conference Profile for an Operator Conference

1 In the *RMX Management* pane, click **Conference Profiles**.

2 In the *Conference Profiles* pane, click the **New Profile** button.
The *New Profile – General* dialog box opens.



3 Define the Profile name and, if required, the Profile general parameters:

Table 10-1 *New Profile - General Parameters*

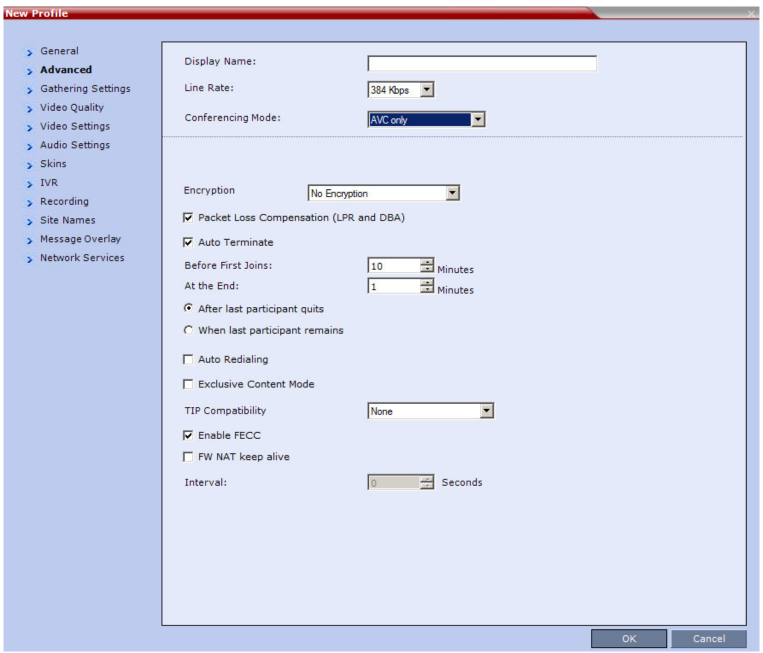
Field/Option	Description
Display Name	Enter a unique Profile name, as follows: • English text uses ASCII encoding and can contain the most characters (length varies according to the field). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. It is recommended to use a name that indicates the Profile type, such as Operator conference or Video Switching conference. **Note:** This is the only parameter that must be defined when creating a new profile.
Routing Name	Enter the Profile name using ASCII characters set. The Routing Name can be defined by the user or automatically generated by the system if no Routing Name is entered as follows: • If an all ASCII text is entered in Display Name, it is used also as the Routing Name. • If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name.
Line Rate	Select the conference bit rate. The line rate represents the combined video, audio and Content rate. The default setting is 384 Kbps.

Table 10-1 *New Profile - General Parameters (Continued)*

Field/Option	Description
Video Switching	If the *Operator Conference* option is selected, this option is disabled, and the selection is cleared. For more information, see "*Video Switching (VSW) Conferencing"* on page **2-4**.
Operator Conference	Select this option to define the profile of an Operator conference. An Operator conference can only be a Continuous Presence conference, therefore when selected, the *High Definition Video Switching* option is disabled and cleared. When defining an *Operator Conference*, the *Send Content to Legacy Endpoints* option in the *Video Settings* tab is cleared and disabled.

4 Click the **Advanced** tab.

The *New Profile – Advanced* dialog box opens.



5 Define the following parameters:

Table 10-2 *New Profile - Advanced Parameters*

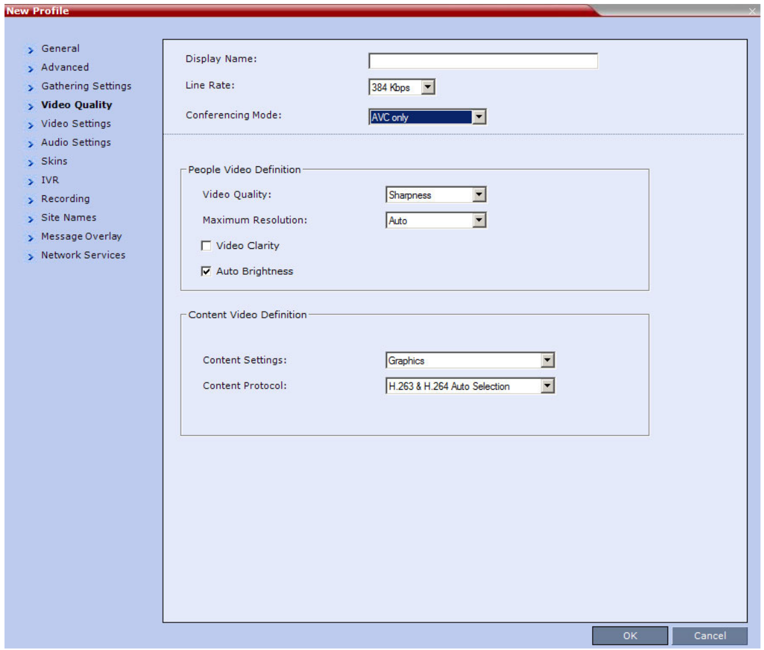
Field/Option	Description
Encryption	Select this check box to activate encryption for the conference. For more information, see "*Media Encryption (AVC Only)"* on page **4-40**.
LPR	When selected (default for CP conferences), *Lost Packet Recovery* creates additional packets that contain recovery information used to reconstruct packets that are lost during transmission. LPR is automatically disabled if High Definition Video Switching is selected. For more information, see "*Packet Loss Compensation (LPR and DBA)"* on page **4-50**.

Table 10-2 *New Profile - Advanced Parameters (Continued)*

Field/Option	Description
Auto Terminate	When selected (default), the conference automatically ends when the termination conditions are met: ***Before First Joins*** — No participant has connected to a conference during the *n* minutes after it started. Default idle time is 10 minutes. ***At the End - After Last Quits*** — All the participants have disconnected from the conference and the conference is idle (empty) for the predefined time period. Default idle time is 1 minute. ***At the End - When Last Participant Remains*** — Only one participant is still connected to the conference for the predefined time period (excluding the recording link which is not considered a participant when this option is selected). This option should be selected when defining a Profile that will be used for Gateway Calls and you want to ensure that the call is automatically terminated when only one participant is connected. Default idle time is 1 minute. **Note:** The selection of this option is automatically cleared and disabled when the *Operator Conference* option is selected. The Operator conference cannot automatically end unless it is terminated by the RMX User.
Echo Suppression	When enabled (default), an algorithm is used to search for and detect echo outside the normal range of human speech (such as echo) and automatically mute them when detected. Clear this option to disable the Echo Suppression algorithm. **Note:** This option is activated only in *MPM+* and MPMx *Card Configuration Mode*.
Keyboard Noise Suppression	When enabled, an algorithm is used to search for and detect keyboard noises and automatically mute them when detected. **Note:** This option is activated only in *MPM+* and MPMx *Card Configuration Mode*.

6 Click the **Video Quality** tab.

The *New Profile – Video Quality* dialog box opens.



7 Define the following parameters:

Table 10-3 *New Profile - Video Quality Parameters*

Field/Option	Description
People Video Definition	
Video Quality	Depending on the amount of movement contained in the conference video, select either: • ***Motion*** – for a higher frame rate without increased resolution • ***Sharpness*** – for higher video resolution and requires more system resources **Note:** When Sharpness is selected as the Video Quality setting in the conference Profile, the RMX will send 4CIF (H.263) at 15fps instead of CIF (H.264) at 30fps. For more information, see *"Video Resolutions in AVC-based CP Conferencing"* on page **3-1**.
Video Clarity™	When enabled (default), *Video Clarity* applies video enhancing algorithms to incoming video streams of resolutions up to and including SD. Clearer images with sharper edges and higher contrast are sent back to all endpoints at the highest possible resolution supported by each endpoint. All layouts, including 1x1, are supported. Video Clarity can only be enabled for Continuous Presence conferences in MPM+ and MPMx Card Configuration Mode.

Table 10-3 New Profile - Video Quality Parameters (Continued)

Field/Option	Description
Content Video Definition	
Content Settings	Select the transmission mode for the Content channel: • ***Graphics*** — basic mode, intended for normal graphics • ***Hi-res Graphics*** — a higher bit rate intended for high resolution graphic display • ***Live Video*** — Content channel displays live video Selection of a higher bit rate for the Content results in a lower bit rate for the people channel. For more information, see "*H.239 / People+Content"* on page **4-2**.
Content Protocol	**H.263** – Content is shared using *H.263* even if some endpoints have *H.264* capability. **Up to H.264** – *H.264* is the default Content sharing algorithm. When selected: • Content is shared using *H.264* if all endpoints have *H.264* capability. • Content is shared using *H.263* if all endpoints do not have *H.264* capability. • Endpoints that do not have at least *H.263* capability can connect to the conference but cannot share Content.

8 Click the **Video Settings** tab.

The *New Profile - Video Settings* dialog box opens.

9 Define the video display mode and layout. For more details, see *Table 2-12, "New AVC Profile - Video Settings Parameters,"* on page **2-30**.

10 Click the **Skins** tab to modify the background and frames.
The *New Profile - Skins* dialog box opens.

11 Select one of the *Skin* options.

12 Click **IVR** tab.

The *New Profile - IVR* dialog box opens.

13 Select the IVR Service and if the conference requires a chairperson.

14 **Optional**. Click the **Recording** tab to enable conference recording with *Polycom RSS 2000*.

15 Define the various recording parameters. for details, see *Table 2-17, "New AVC Profile - Recording Parameters,"* on page **2-40**.

16 Click **OK** to complete the *Profile* definition.
A new *Profile* is created and added to the *Conference Profiles* list.

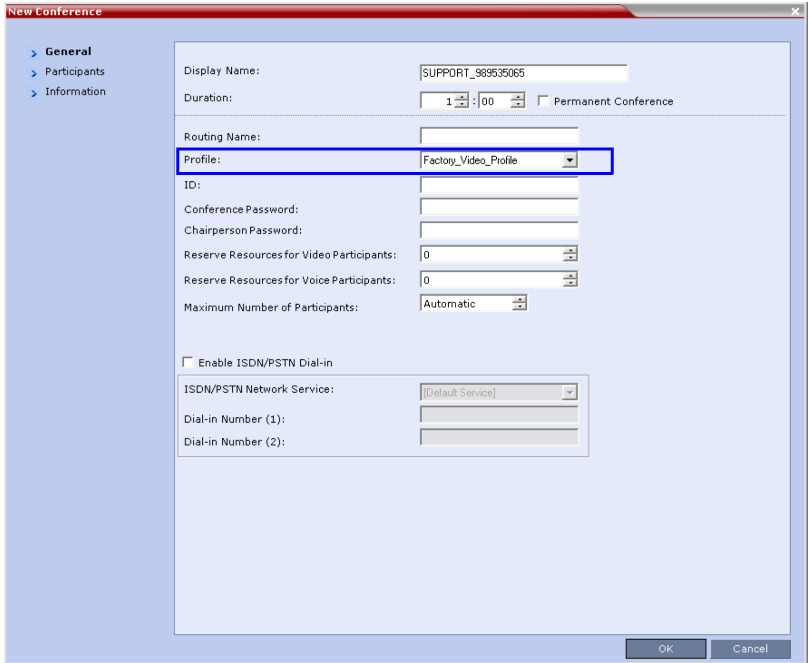
Defining an Ongoing Operator Conference

To start a conference from the Conference pane:

1 In the *Conferences* pane, click the **New Conference** ( ) button.

The *New Conference – General* dialog box opens.

2 In the *Profile* field, select a Profile in which the *Operator Conference* option is selected.



Upon selection of the Operator Conference Profile, the *Display Name* is automatically taken from the RMX User *Login Name*. This name cannot be modified.

Only one Operator conference can be created for each User Login name.

3 Define the following parameters:

***Table 10-4** New Conference – General Options*

Field	Description
Duration	Define the duration of the conference in hours using the format HH:MM (default 01:00). **Notes:** • The Operator conference is automatically extended up to a maximum of 168 hours. Therefore, the default duration can be used. • This field is displayed in all tabs.

Table 10-4 *New Conference – General Options (Continued)*

Field	Description
Routing Name	*Routing Name* is the name with which ongoing conferences, Meeting Rooms, Entry Queues and SIP Factories register with various devices on the network such as gatekeepers and SIP servers. This name must be defined using ASCII characters. **Comma, colon and semicolon characters cannot be used in the *Routing Name*.** The *Routing Name* can be defined by the user or automatically generated by the system if no *Routing Name* is entered as follows: • If ASCII characters are entered as the *Display Name*, it is used also as the *Routing Name* • If a combination of Unicode and ASCII characters (or full Unicode text) is entered as the *Display Name*, the *ID* (such as Conference ID) is used as the *Routing Name*. If the same name is already used by another conference, Meeting Room or Entry Queue, the RMX displays an error message and requests that you to enter a different name.
ID	Enter the unique-per-MCU conference ID. If left blank, the MCU automatically assigns a number once the conference is launched. This ID must be communicated to conference participants to enable them to dial in to the conference.
Conference Password	Leave this field empty when defining an Operator conference.
Chairperson Password	Leave this field empty when defining an Operator conference.
Reserve Resources for Video Participants	Enter the number of video participants for which the system must reserve resources. Default: 0 participants. When defining an Operator conference it is recommended to reserve resources for at least 2 video participants (for the operator and one additional participant - who will be moved to the Operator conference for assistance).
Reserve Resources for Audio Participants	Enter the number of audio participants for which the system must reserve resources. Default: 0 participants. When defining an Operator conference and the operator is expected to help voice participants, it is recommended to reserve resources for at least 2 video participants (for the operator and one additional participant - who will be moved to the Operator conference for assistance).
Maximum Number of Participants	Enter the maximum number of participants that can connect to an Operator conference (you can have more than two), or leave the default selection (Automatic). Maximum number of participants that can connect to an Operator conference:

Table 10-4 New Conference – General Options (Continued)

Field	Description
Enable ISDN/PSTN Dial-in	Select this check box if you want ISDN and PSTN participants to be able to connect directly to the Operator conference. This may be useful if participants are having problems connecting to their conference and you want to identify the problem or help them connect to their destination conference.
ISDN/PSTN Network Service and Dial-in Number	If you have enable the option for ISDN/PSTN direct dial-in to the Operator conference, assign the ISDN/PSTN Network Service and a dial-in number to be used by the participants, or leave these fields blank to let the system select the default Network Service and assign the dial-in Number. **Note:** The dial-in number must be unique and it cannot be used by any other conferencing entity.

4 Click the **Participants** tab.
The *New Conference - Participants* dialog box opens.

You must define or add the Operator participant to the Operator conference.

This participant must be defined as a **dial-out** participant.

Define the parameters of the endpoint that will be used by the RMX User to connect to the Operator conference and to other conference to assist participants.

For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Participants Tab"* on page 3-17.

5 **Optional**. Click the **Information** tab**.**
The *Information* tab opens.

6 Enter the required information. For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Information Tab"* on page 3-20.

7 Click **OK**.

The new Operator conference is added to the ongoing *Conferences* list with a special icon .

The Operator participant is displayed in the *Participants* list with an Operator participant icon , and the system automatically dials out to the Operator participant.

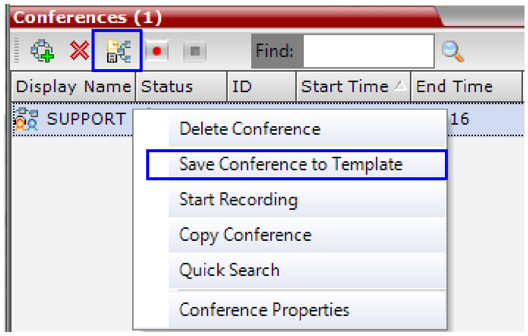
Saving an Operator Conference to a Template

The Operator conference that is ongoing can be saved as a template.

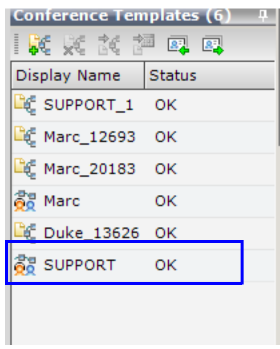
To save an ongoing Operator conference as a template:

1 In the *Conferences List*, select the Operator conference you want to save as a Template.

2 Click the **Save Conference to Template** () button.
or
Right-click and select **Save Conference to Template**.



The conference is saved to a template whose name is taken from the ongoing conference *Display Name* (the Login name of the RMX User). The Template is displayed with the Operator Conference icon.



Starting an Operator Conference from a Template

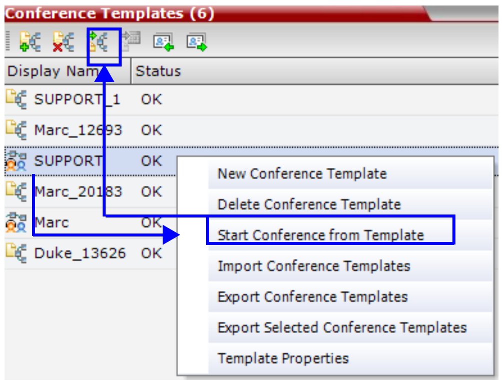
An ongoing Operator conference can be started from an Operator Template saved in the *Conference Templates* list.

To start an ongoing Operator conference from an Operator Template:

1 In the *Conference Templates* list, select the Operator Template to start as an ongoing Operator conference.

- You can only start an Operator conference from a template whose name is identical to your Login Name. For example, if your Login name is Polycom, you can only start an Operator conference from a template whose name is Polycom.
- If an ongoing Operator conference with the same name or any other conference with the same ID is already running, you cannot start another Operator conference with the same login name.

2 Click the **Start Conference from Template** ( ) button.
or
Right-click and select **Start Conference from Template**.



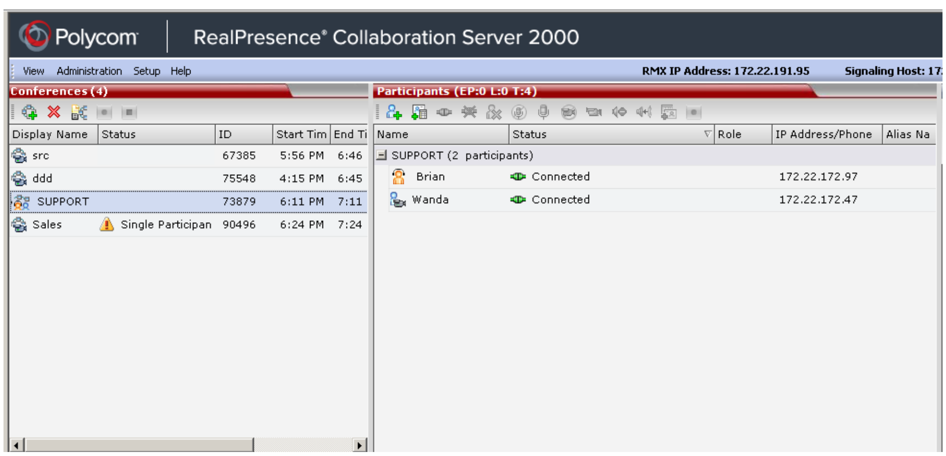
The conference is started.

The name of the ongoing conference in the *Conferences* list is taken from the Conference Template *Display Nam*e.

Monitoring Operator Conferences and Participants Requiring Assistance

Operator conferences are monitored in the same way as standard ongoing conferences.

Each Operator conference includes at least one participant - the Operator.



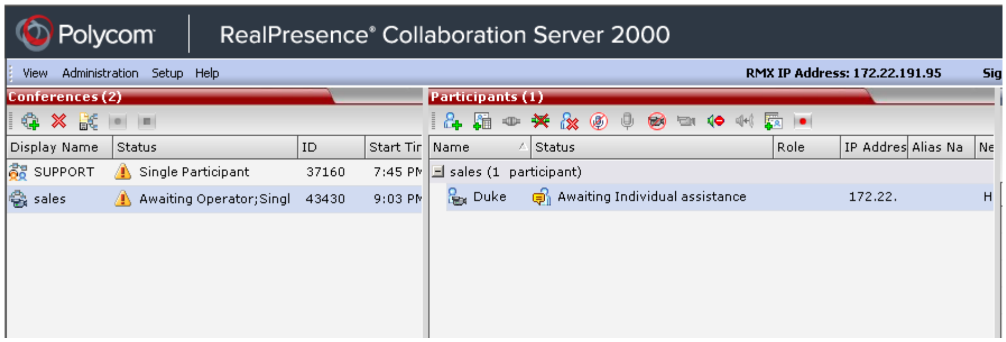
You can view the properties of the *Operator conference* by double-clicking the conference entry in the *Conferences* list or by right-clicking the conference entry and selecting **Conference Properties**. For more information, see the *RealPresence Collaboration Server 1500/ 2000/4000 Getting Started Guide*, "*Conference Level Monitoring"* on page **3-41**.

Requesting Help

A participant can request help using the appropriate DTMF code from his/her touch tone telephone or the endpoint's DTMF input device. The participant can request *Individual Assistance* (default DTMF code ***0**) or *Conference Assistance* (default DTMF code **00**).

Participants in Entry Queues who failed to enter the correct destination conference ID or the conference password will wait for operator assistance (provided that an Operator conference is active).

When requiring or requesting operator assistance, the RMX management application displays the following:



- The participant's connection *Status* changes, reflecting the help request. For more information, see Table 10-5.
- The conference status changes and it is displayed with the exclamation point icon and the status "Awaiting Operator".
- The appropriate voice message is played to the relevant participants indicating that assistance will be provided shortly.

The following icons and statuses are displayed in the *Participant Status* column:

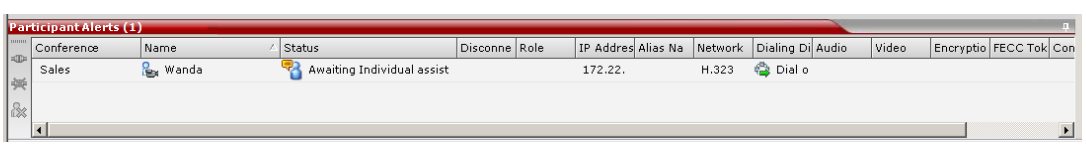
Table 10-5 *Participants List Status Column Icons and Indications*

Icon	Status Indication	Description
	*Awaiting Individual Assistance*	The participant has requested the operator's assistance for himself/herself.
	*Awaiting Conference Assistance*	The participant has requested the operator's assistance for the conference. Usually this means that the operator is requested to join the conference.

When the Operator moves the participant to the *Operator conference* for individual assistance the participant Status indications are cleared.

Participant Alerts List

The *Participant Alerts* list contains all the participants who are currently waiting for operator assistance.



Participants are automatically added to the *Participants Alerts* list in the following circumstances:

- The participant fails to connect to the conference by entering the wrong conference ID or conference password and waits for the operator's assistance
- The participant requests Operator's Assistance during the ongoing conference

This list is used as reference only. Participants can be assisted and moved to the *Operator conference* or the destination conference only from the *Participants* list of the Entry Queues or ongoing conference where they are awaiting assistance.

The participants are automatically removed from the *Participant Alerts* list when moved to any conference (including the *Operator conference*).

Audible Alarms

In addition to the visual cues used to detect events occurring on the RMX, an audible alarm can be activated and played when participants request Operator Assistance.

Using Audible Alarms

The Audible Alarm functionality for Operator Assistance requests is enabled for each MCU in either the RMX Web Client or RMX Manager.

The Audible Alarm played when Operator Assistance is requested is enabled and selected in the **Setup > Audible Alarm > User Customization**. When the Audible Alarm is activated, the *.wav file selected in the *User Customization* is played, and it is repeated according to the number of repetitions defined in the *User Customization*.

If more than one RMX is monitored in the *RMX Manager*, the Audible Alarm must be enabled separately for each RMX installed in the site/configuration. A different *.wav file can be selected for each MCU.

When multiple Audible Alarms are activated in different conferences or by multiple MCUs, the Audible Alarms are synchronized and played one after the other. It is important to note that when *Stop Repeating Alarm* is selected from the toolbar from the RMX Web Client or RMX Manager, all activated Audible Alarms are immediately halted.

For more details on Audible alarms and their configuration, see "*Audible Alarms"* on page **21-43**.

Moving Participants Between Conferences

The RMX User can move participants between ongoing conferences, including the *Operator conference*, and from the Entry Queue to the destination conference if help is required.

When moving between conferences or when a participant is moved from an Entry Queue to a conference by the RMX user (after failure to enter the correct destination ID or conference password), the IVR messages and slide display are skipped.

Move Guidelines

- Move is available only between CP conferences. Move is unavailable from/to Video Switching conferences.
- Move between conferences can be performed without an active *Operator conference*.
- When moving the conference chairperson from his/her conference to another conference, the source conference will automatically end if the *Auto Terminate When Chairperson Exits* option is enabled and that participant is the only conference chairperson.
- When moving the Operator to any conference (following assistance request), the IVR messages and slide display are skipped.

- Participants cannot be moved from a Telepresence conference.
- Participants cannot be moved from LPR-enabled conferences to non-LPR conferences. Move from non-LPR conferences to LPR-enabled conferences is available.
- Move between encrypted and non-encrypted conferences depends on the **ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF** flag setting, as described in Table 10-6:

Table 10-6 *Participant Move Capabilities vs. ALLOW_NON_ ENCRYPT_PARTY_IN_ENCRYPT_CONF flag setting*

Flag Setting	Source Conference/ EQ Encrypted	Destination Conference Encrypted	Move Enabled?
NO	Yes	Yes	Yes
NO	Yes	No	Yes
NO	No	Yes	No
NO	No	No	Yes
YES	Yes	Yes	Yes
YES	Yes	No	Yes
YES	No	Yes	Yes
YES	No	No	Yes

- When moving dial-out participants who are disconnected to another conference, the system automatically dials out to connect them to the destination conference.
- Cascaded links cannot be moved between conferences.
- Participants cannot be moved to a conference if the move will cause the number of participants to exceed the maximum number of participants allowed for the destination conference.

Moving Participants

RMX users can assist participants by performing the following operations:

- Move a participant to an *Operator conference* (Attend a participant).
- Move a participant to the Home (destination) conference.
- Move participant from one ongoing conference to another

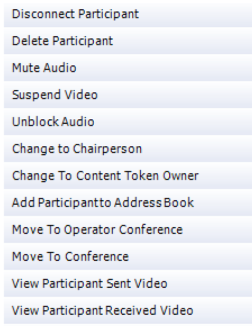
A move can be performed using the following methods:

- Using the participant right-click menu
- Using drag and drop

To move a participant from the ongoing conference using the right-click menu options:

1. In the *Conferences* list, click the conference where there are participants waiting for Operator's Assistance to display the list of participants.

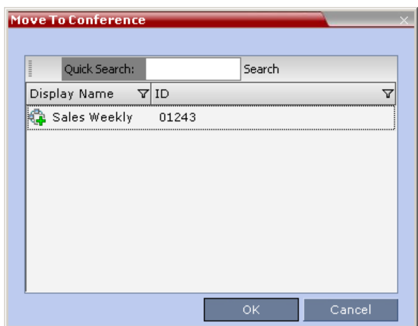
2 In the *Participants* list, right-click the icon of the participant to move and select one of the following options:



— **Move to Operator Conference** - to move the participant to the Operator conference.

— **Move to Conference** - to move the participant to any ongoing conference.

When selected, the *Move to Conference* dialog box opens, letting you select the name of the destination conference.



— **Back to Home Conference** - if the participant was moved to another conference or to the *Operator conference*, this options moves the participant back to his/her source conference.

This option is not available if the participant was moved from the Entry Queue to the *Operator conference* or the destination conference.

Moving a Participant Interactively

You can drag and drop a participant from the Entry Queue or ongoing conference to the Operator or destination (Home) conference:

1 Display the participants list of the Entry Queue or the source conference by clicking its entry in the *Conferences* list.

2 In the Participants list, drag the icon of the participant to the *Conferences List* pane and drop it on the *Operator Conference* icon or another ongoing conference.

11

Conference Templates

Conference Templates enable administrators and operators to create, save, schedule and activate identical conferences.

A *Conference Template*:

- Saves the conference Profile.
- Saves all participant parameters including their *Personal Layout* and *Video Forcing* settings.
- Simplifies the setting up *Telepresence* conferences where precise participant layout and video forcing settings are crucial.

Guidelines

- The maximum number of templates is:
  - RealPresence Collaboration Server (RMX) 1500 — 100
  - RealPresence Collaboration Server (RMX) 2000 — 100
  - RealPresence Collaboration Server (RMX) 4000 — 200
- A maximum of 200 participants can be saved in a *Conference Template* when the RMX is in MPM+ or MPMx mode. When the RMX is in MPM (RealPresence Collaboration Server (RMX) 2000) mode, the maximum is 80 participants.
- If the RMX is switched to from MPM+ or MPMx mode to MPM (RealPresence Collaboration Server (RMX) 2000) mode, conference templates may include more participants than the allowed maximum in MPM mode.

  Trying to start a *Conference Template* that exceeds the allowed maximum number of participants will result in participants being disconnected due to resource deficiency.

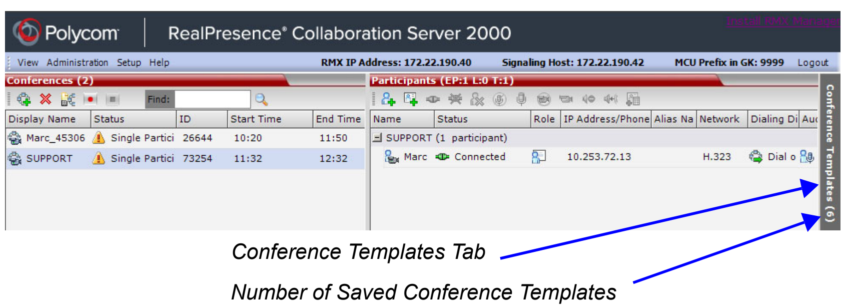
From *Version 7.1*, *MPM* media cards are not supported.

- If the Profile assigned to a conference is deleted while the conference is ongoing the conference cannot be saved as a template.
- A Profile assigned to a *Conference Template* cannot be deleted. The system does not permit such a deletion.
- Profile parameters are not embedded in the *Conference Template*, and are taken from the Profile when the *Conference Template* becomes an ongoing conference. Therefore, any changes to the Profile parameters between the time the *Conference Template* was created and the time that it is activated (and becomes an ongoing conference) will be applied to the conference.
- Only defined participants can be saved to the *Conference Template*. Before saving a conference to a template ensure that all undefined participants have disconnected.
- Undefined participants are not saved in *Conference Templates*.

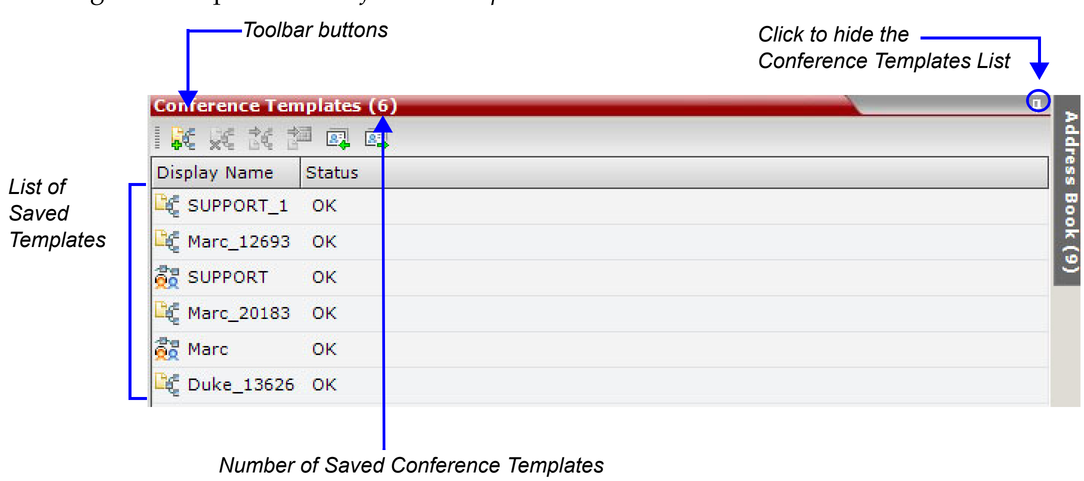
- Participant properties are embedded in the *Conference Template* and therefore, if the participant properties are modified in the Address Book after the *Conference Template* has been created they are not applied to the participant whether the *Template* becomes an ongoing conference or not.
- The *Conference Template* display name, routing name or ID can be the same as an Ongoing Conference, reservation, Meeting Room or Entry Queue as it is not active. However, an ongoing conference cannot be launched from the *Conference Template* if an ongoing conference, Meeting Room or Entry Queue already has the same name or ID. Therefore, it is recommended to modify the template ID, display name, routing name to be unique.
- A *Reservation* that has become an ongoing conference can be saved as *Conference Template*.
- SIP Factories and Entry Queues cannot be saved as *Conference Templates*.
- The conference specified in the *Conference Template* can be designated as a *Permanent Conference*. For more information see "*Lecture Mode (AVC Only)"* on page **4-73**.

Using Conference Templates

The *Conference Templates* list is initially displayed as a closed tab in the *RMX Web Client* main window. The number of saved *Conference Templates* is indicated on the tab.



Clicking the tab opens the *Conference Templates* list.



The *Conference Templates* are listed by *Conference Template Display Name* and *ID* and can be sorted by either field. The list can be customized by re-sizing the pane, adjusting the column widths or changing the order of the column headings.

For more information see *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide, "Customizing the Main Screen"* on page **10**.

Clicking the anchor pin ( ) button hides the *Conference Templates* list as a closed tab.

Toolbar Buttons

The *Conference Template* toolbar includes the following buttons:

***Table 1** Conference Templates – Toolbar Buttons*

Button	Description
New Conference Template	Creates a new Conference Template.
Delete Conference Template	Deletes the Conference Template(s) that are selected in the list.
Start Conference from Template	Starts an ongoing conference from the *Conference Template* that has an identical name, ID parameters and participants as the template.
Schedule Reservation from Template	Creates a conference Reservation from the Conference Template with the same name, ID, parameters and participants as the Template. Opens the *Scheduler* dialog box enabling you to modify the fields required to create a single or recurring *Reservation* based on the template. For more information see "*Reservations"* on page **9-1**.

The ***Conferences List*** toolbar includes the following button:

***Table 2** Conferences List – Toolbar Button*

Button	Description
Save Conference to Template	Saves the selected ongoing conference as a Conference Template.

Creating a New Conference Template

There are two methods to create a *Conference Template*:

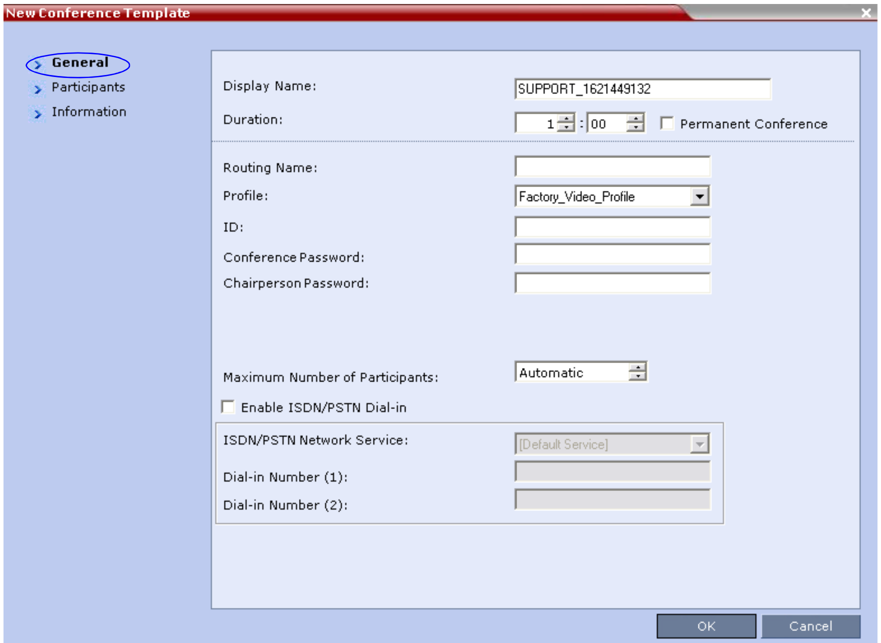
- From scratch - defining the conference parameters and participants
- Saving an ongoing conference as Template

Creating a new Conference Template from Scratch

To create a new Conference Template:

1. In the *RMX Web Client*, click the **Conference Templates** tab.
2. Click the **New Conference Template** ( ) button.

The *New Conference Template - General* dialog box opens.



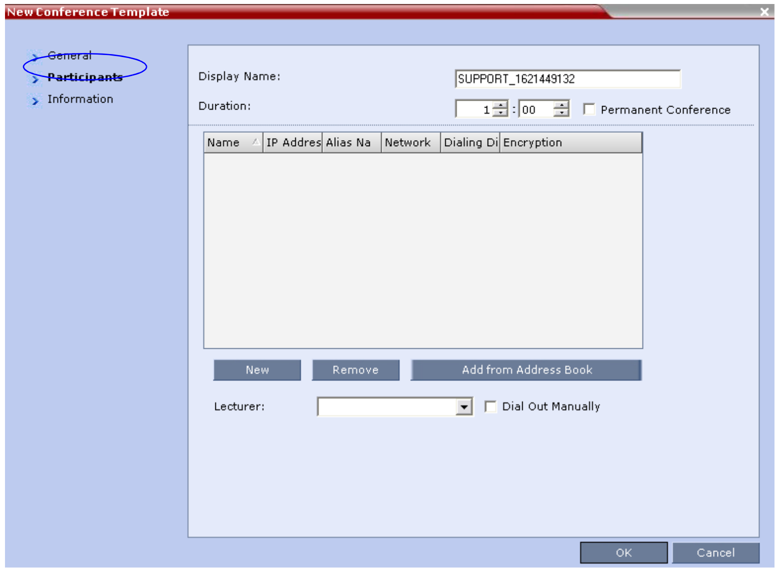
3 The fields of the *New Template – General* dialog box are identical to those of the *New Conference – General* dialog box. For a full description of the fields see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide,* "*General Tab"* on page **3-14**.

4 Modify the fields of the *General* tab.

> A unique dial-in number must be assigned to each conferencing entity. However, Conference Templates can be assigned dial-in numbers that are already assigned to other conferencing entities, but when the template is used to start an ongoing conference or schedule a reservation, it will not start if another ongoing conference, Meeting Room, Entry Queue or Gateway Profile is using this number.

5 Click the **Participants** tab.

The *New Template – Participants* dialog box opens.



The fields of the *New Template – Participants* dialog box are the same as those of the *New Conference – Participant* dialog box.

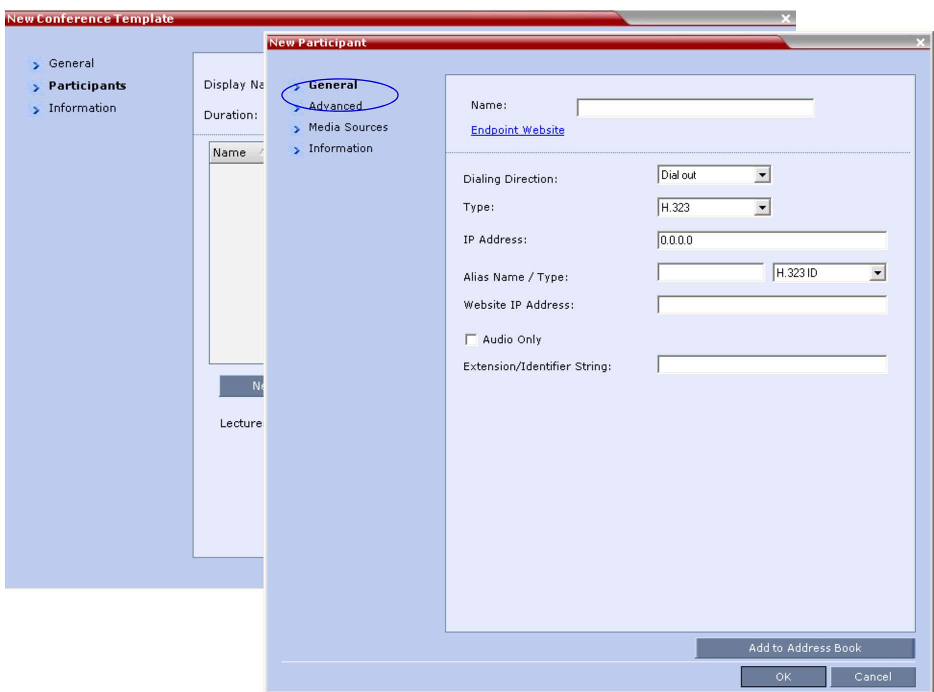
For a full description of these fields see the *RealPresence Collaboration Server 1500/2000/ 4000 Getting Started Guide, "Participants Tab"* on page **3-17**.

6 **Optional.** Add participants to the template from the *Address Book*.

7 Click the **New** button.

The *New Participant – General* tab opens.

The *New Template – Participant* dialog box remains open in the background.

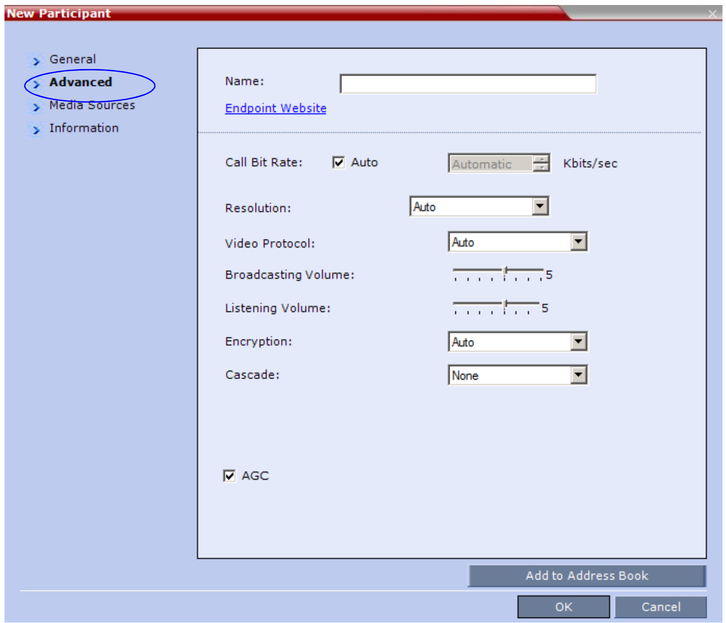


For a full description of the *General* tab fields see *"Adding a new participant to the Address Book Directly"* on page 8.

8 Modify the fields of the *General* tab.

9 Click the **Advanced** tab.

The *New Participant – Advanced* tab opens.

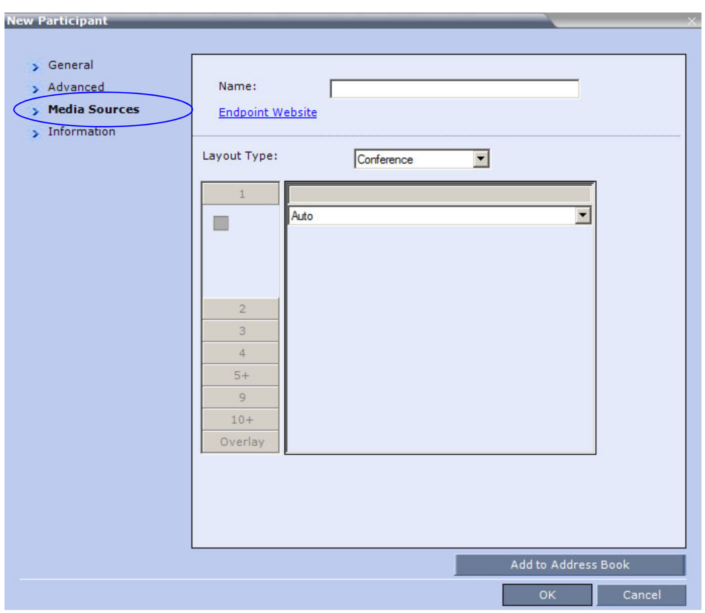


For a full description of the *Advanced* tab fields see, *"New Participant – Advanced Properties"* on page 12.

10 Modify the fields of the *Advanced* tab.

11 Click the **Media Sources** tab.

The *Media Sources* tab opens.



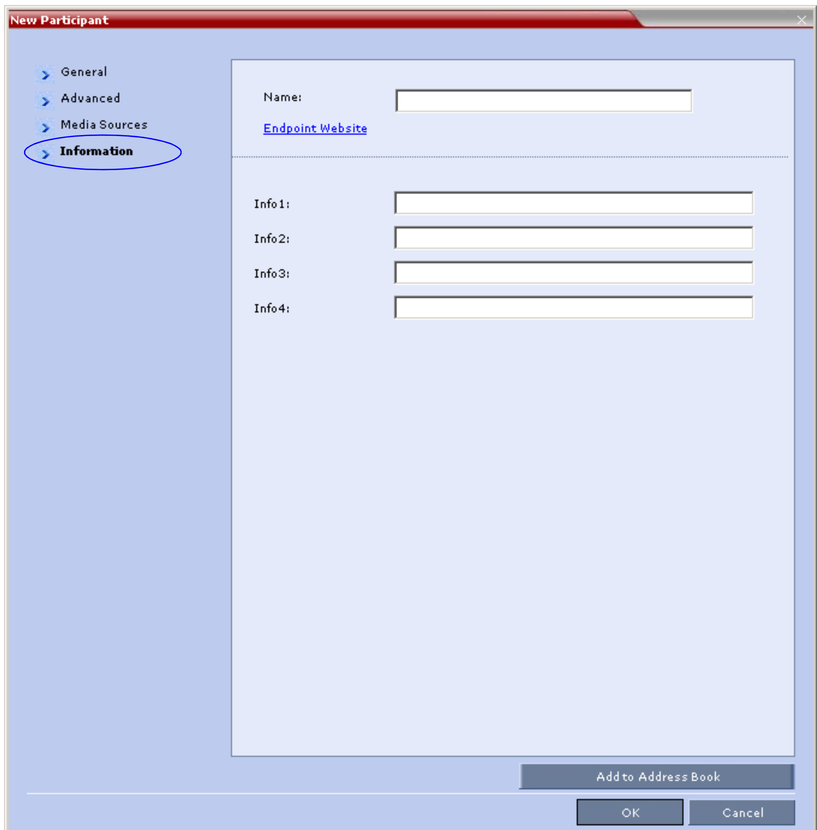
The *Media Sources* tab enables you to set up and save *Personal Layout* and *Video Forcing* settings for each participant. This is especially important when setting up *Telepresence* conferences.

For a full description of *Personal Layout* and *Video Forcing* settings see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide, "Changing the Video Layout of a Conference (AVC-Based Conferences)"* on page **3-56** and "*Video Forcing (AVC-based Conferences)"* on page **3-58**.

12 Modify the *Personal Layout* and *Video Forcing* settings for the participant.

13 **Optional.** Click the **Information** tab.

The *New Participant – Information* tab opens.



For a full description of the *Information* fields see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide, "Information Tab"* on page **3-20**.

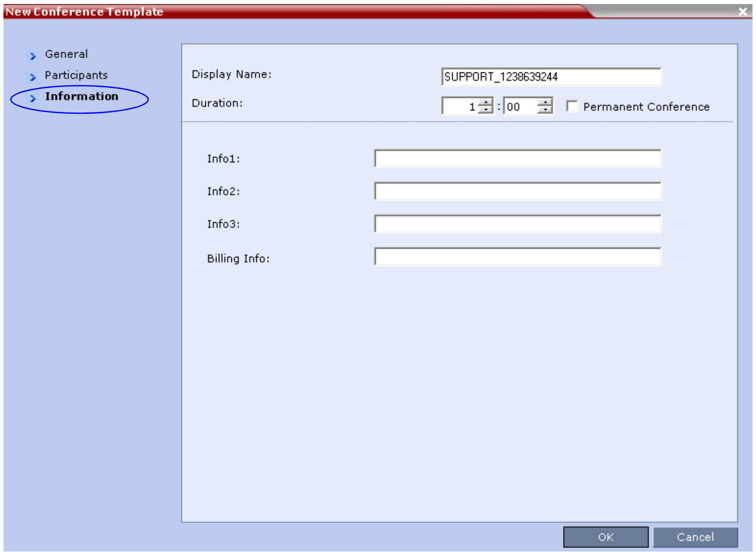
14 Click the **OK** button.

The participant you have defined is added to the *Participants List*.

The New Participant dialog box closes and you are returned to the *New Template – Participant* dialog box (which has remained open since Step 7).

15 **Optional.** In the *New Conference Template* dialog box, click the **Information** tab.

The *New Conference Template – Information* tab opens.



For a full description of the *Information* fields see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide, "Information Tab"* on page **20**.

16 Click the **OK** button.

The *New Conference Template* is created and its name is added to the *Conference Templates* list.

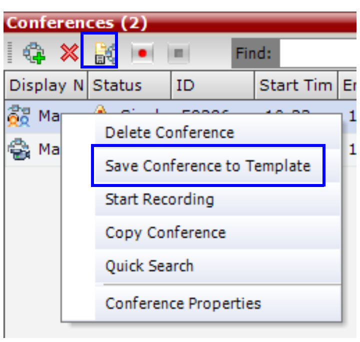
Saving an Ongoing or AVC-based Operator Conference as a Template

Any ongoing or AVC-based *Operator Conference* can be saved as a template.

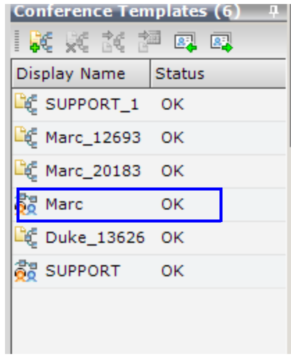
To save an ongoing or AVC-based Operator Conference as a template:

1 In the *Conferences List*, select the conference or *Operator Conference* to be saved as a Template.

2 Click the **Save Conference to Template** () button.
or
Right-click and select **Save Conference to Template**.



The conference is saved to a template whose name is taken from the ongoing conference *Display Name* (the *Login* name of the *RMX User*). The *Template* is displayed with the *Operator Conference* icon.



Conference Templates saved from an ongoing conference does not include *Message Overlay* text messages.

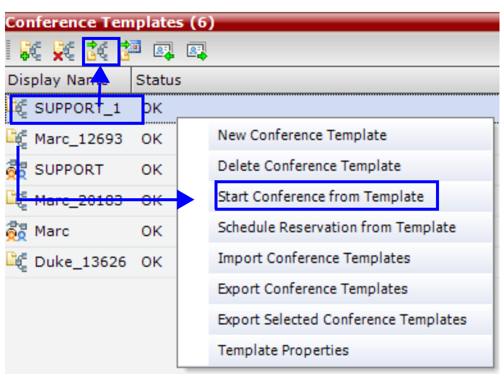
Starting an Ongoing Conference From a Template

An ongoing conference can be started from any Template saved in the *Conference Templates* list. In SVC-based templates, only defined dial-in participants may be part of the conference.

To start an ongoing conference from a Template:

1 In the *Conference Templates* list, select the Template you want to start as an ongoing conference.

2 Click the **Start Conference from Template** ( ) button.
or
Right-click and select **Start Conference from Template**.



The conference is started.

> If a Conference Template is assigned a dial-in number that is already assigned to an ongoing conference, Meeting Room, Entry Queue or Gateway Profile, when the template is used to start an ongoing conference or schedule a reservation it will not start. However, the same number can be assigned to several conference templates provided they are not used to start an ongoing conference at the same time. If a dial in number conflict occurs prior to the conference's start time, an alert is displayed: "ISDN dial-in number is already assigned to another conferencing entity" and the conference cannot start.

The name of the ongoing conference in the *Conferences* list is taken from the Conference Template *Display Nam*e.

Participants that are connected to other ongoing conferences when the template becomes an ongoing conference are not connected.

> If an ongoing conference, Meeting Room or Entry Queue with the same *Display Name, Routing Name* or *ID* already exist in the system, the conference will not be started.

> Conference Templates saved from an ongoing conference does not include *Message Overlay* text messages.

Starting an Operator Conference from a Template (AVC Conferencing)

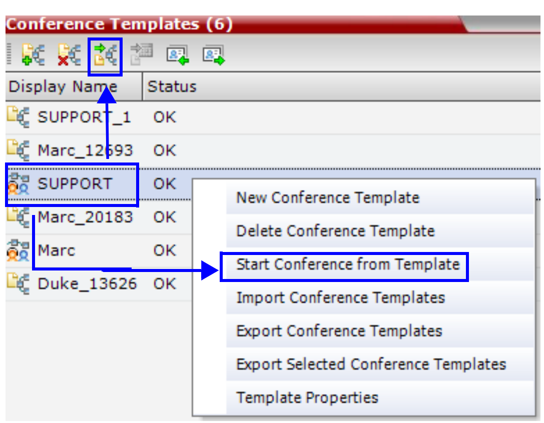
An ongoing Operator conference can be started from an Operator Template saved in the *Conference Templates* list.

To start an ongoing Operator conference from an Operator Template:

1 In the *Conference Templates* list, select the Operator Template to start as an ongoing Operator conference.

> - You can only start an Operator conference from a template whose name is identical to your Login Name. For example, if your Login name is Polycom, you can only start an Operator conference from a template whose name is Polycom.
> - If an ongoing Operator conference with the same name or any other conference with the same ID is already running, you cannot start another Operator conference with the same login name.

2 Click the **Start Conference from Template** ( ) button.
or
Right-click and select **Start Conference from Template**.



The conference is started.

The name of the ongoing conference in the *Conferences* list is taken from the Conference Template *Display Name*.

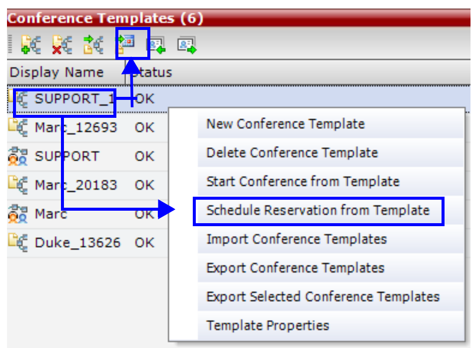
Scheduling a Reservation From a Conference Template (AVC Conferencing)

A *Conference Template* can be used to schedule a single or recurring *Reservation*.

To schedule a Reservation from a Conference Template:

1 In the *Conference Templates* list, select the Conference Template you want to schedule as a Reservation.

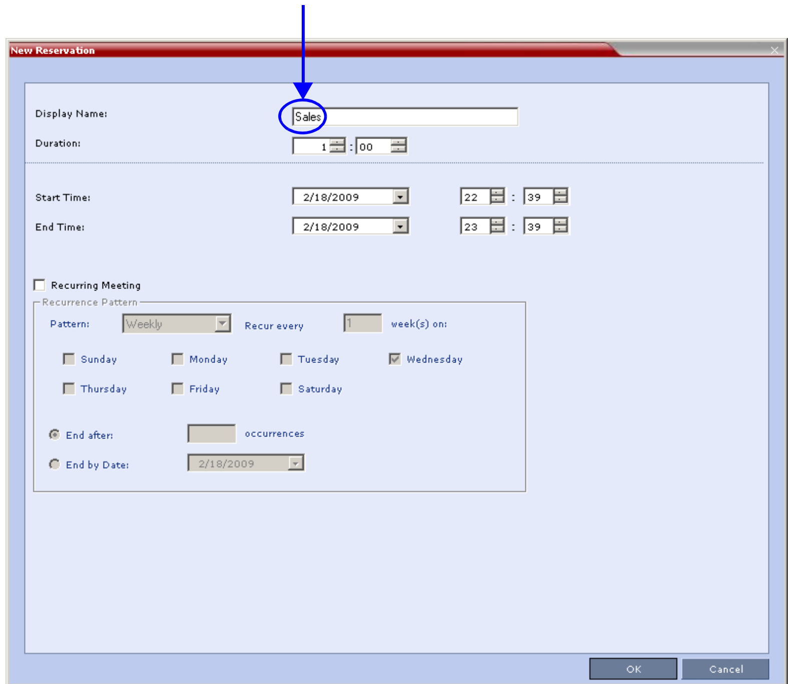
2 Click the **Schedule Reservation from Template** ( ) button.
or
Right-click and select **Schedule Reservation from Template**.



The *Reservation Properties* dialog box is displayed.

The *Display Name* of the *Reservation* is taken from the Conference Template *Display Name*.

Conference Template and Reservation Name



For a full description of the *Reservation Properties* fields see Table 9-3, *"New Reservation – Schedule Tab,"* on page **9-11**.

3 Modify the fields of the *Reservation Properties*.

4 Click the **OK** button.

A *Reservation* is created based on the *Conference Template*. The *Reservation* can be viewed and modified along with all other *Reservations* using the *Reservations - Calendar View* and *Reservations List*.

If you create a recurring reservation all occurrences have the same ID. A recurring Reservation is assigned the same ISDN/PSTN dial-in number for all recurrences.

If a dial-in number conflict occurs prior to the conference's start time, an alert is displayed: "ISDN dial-in number is already assigned to another conferencing entity" and the conference cannot start.

The series number (`_0000n`) of each reservation is appended to its *Display Name*.

Example:

Conference Template name: `Sales`

Display Name for single scheduled occurrence: `Sales`

If 3 recurrences of the reservation are created:

Display Name for occurrence 1: `Sales`**`_00001`**

Display Name for occurrence 2: `Sales_`**`00002`**

Display Name for occurrence 3: `Sales_`**`00003`**

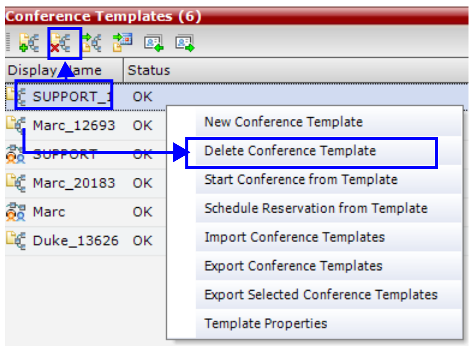
Deleting a Conference Template

One or several *Conference Templates* can be deleted at a time.

To delete Conference Templates:

1 In the *Conference Templates* list, select the *Template(s)* you want to delete.

2 Click the **Delete Conference Template** ( ) button.
or
Right-click and select **Delete Conference Template**.



A confirmation dialog box is displayed.

3 Click the **OK** button to delete the *Conference Template(s)*.

Exporting and Importing Conference Templates

Conference Templates can be exported from one MCU and imported to multiple MCUs in your environment. Additionally, you can export *Conference Templates* and their associated *Conference Profiles* simultaneously. Using this option can save configuration time and ensures that identical settings are used for conferences running on different MCUs. This is especially important in environments using cascading conferences that are running on different MCUs.

Guidelines

- Administrators can export and import *Conference Templates*. Operators are only allowed to export *Conference Templates*.
- You can select a single, multiple or all *Conference Templates* to be exported.
- Both *Conference Templates* and their associated *Conference Profiles* can be exported and imported simultaneously when enabling the **Export includes conference profiles** or **Import includes conference profiles** options.
- Exporting and importing *Conference Templates* only can be used when you want to export and import individual *Conference Templates* without their associated Conference Profiles. This option enables you to import *Conference Templates* when *Conference Profiles* already exist on an MCU.

Exporting Conference Templates

Conference Templates are exported to a single XML file that can be used to import the *Conference Templates* on multiple MCUs.

Using the *Export Conference Templates* option, you can:

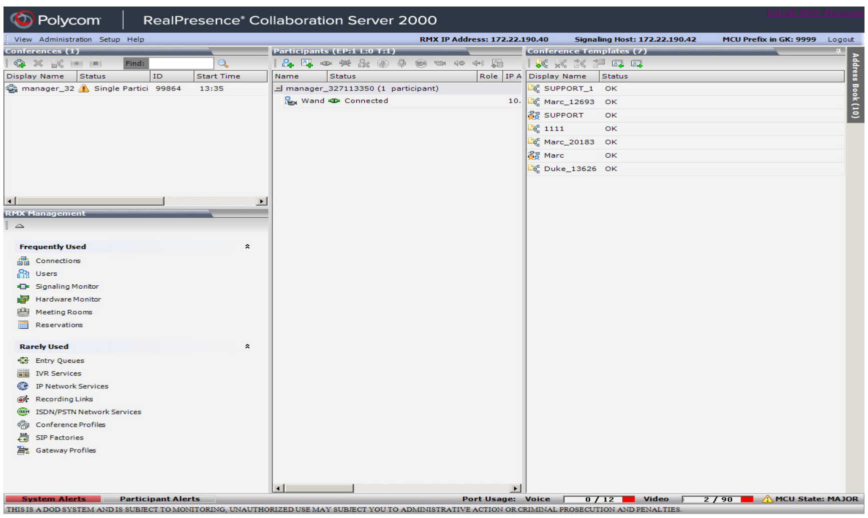
- Export all *Conference Templates* from an MCU
- Export selected *Conference Templates*

Exporting All Conference Templates from an MCU

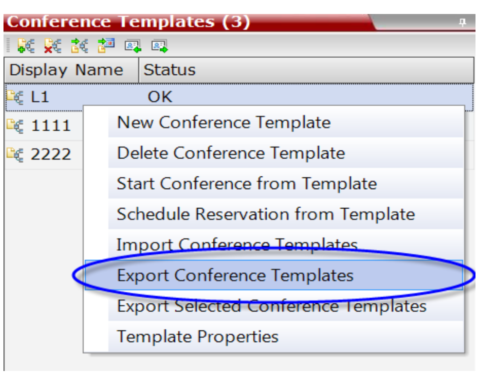
To export all Conference Templates from an MCU:

1 In the *RMX Web Client* main window, click the *Conference Templates* tab.

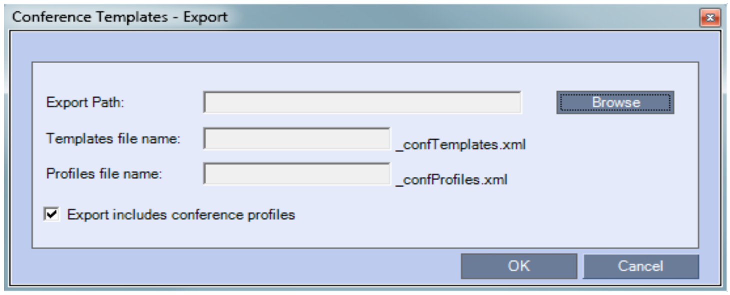
The *Conference Templates* list pane is displayed.



2 Click the **Export Conference Templates**  button or right-click the *Conference Templates* list, and then click **Export Conference Templates**.



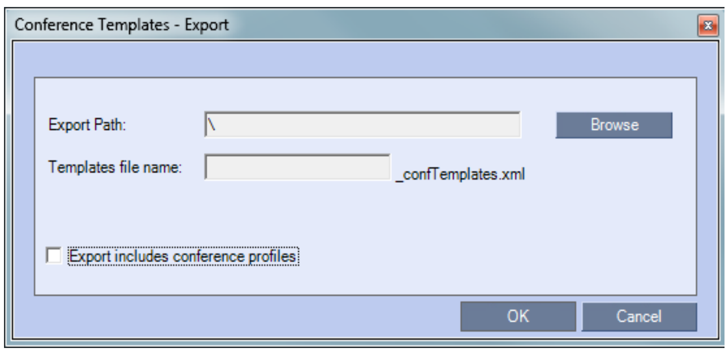
The *Conference Templates - Export* dialog box is displayed.



3 In the *Export Path* field, type the path name to the location where you want to save the exported file or click **Browse** to select the desired path.

4 Optional. Clear the **Export includes conference profiles** check box when you only want to export *Conference Templates*.

When this check box is cleared, the *Conference Templates - Export* dialog box is displayed without the *Profiles file name* field.



5 In the *Templates file name* field, type the file name prefix. The file name suffix (_confTemplates.xml) is predefined by the system. For example, if you type *Templates01*, the exported file name is defined as *Templates01_confTemplates.xml*.

The system automatically defines the *Profiles file name* field with the same file name prefix as the *Templates file name* field. For example, if you type *Templates01* in the *Templates file name* field, the exported profiles file name is defined as *Templates01_confProfiles.xml*.

6 Click **OK** to export the *Conference Templates* and *Conference Profiles* to a file.

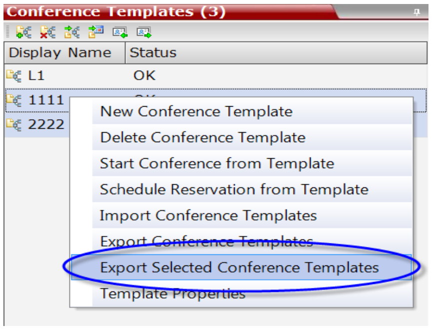
Exporting Selected Conference Templates

You can export a single *Conference Template* or multiple *Conference Templates* to other MCUs in your environment.

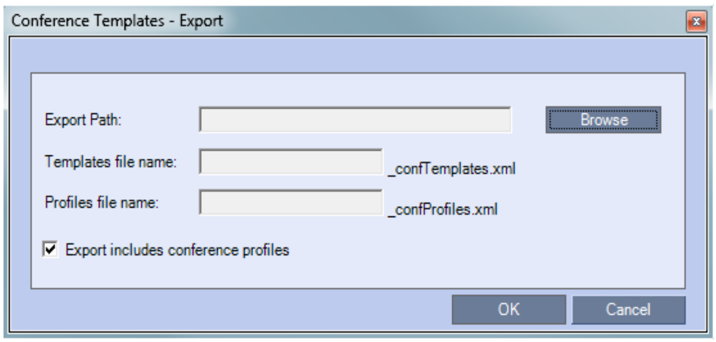
To export selected Conference Templates:

1 In the *Conference Templates* list, select the templates you want to export.

2 Right-click the *Conference Templates* to be exported, and then click **Export Selected Conference Templates**.



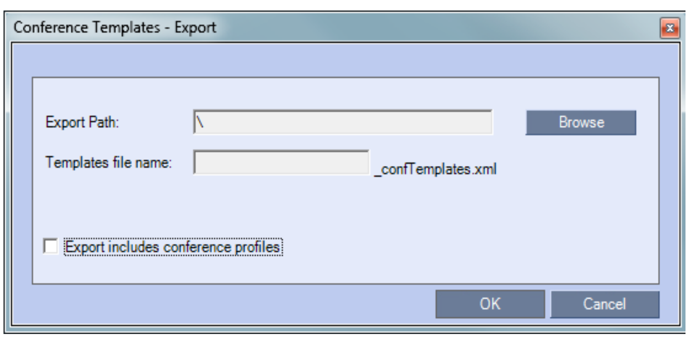
The *Conference Templates - Export* dialog box is displayed.



3 In the *Export Path* field, type the path name to the location where you want to save the exported file or click **Browse** to select the desired path.

4 Optional. Clear the **Export includes conference profiles** check box when you only want to export Conference Templates.

When this check box is cleared, the *Conference Templates - Export* dialog box is displayed without the *Profiles file name* field.



5 In the *Templates file name* field, type the file name prefix. The file name suffix (_confTemplates.xml) is predefined by the system. For example, if you type, *Templates01*, the exported file name is defined as *Templates01_confTemplates.xml*.

The system automatically defines the *Profiles file name* field with the same file name prefix as the *Templates file name* field. For example, if you type *Templates01* in the *Templates file name* field, the exported profiles file name is defined as *Templates01_confProfiles.xml*.

6 Click **OK** to export the *Conference Templates* and *Conference Profiles* to a file.

Importing Conference Templates

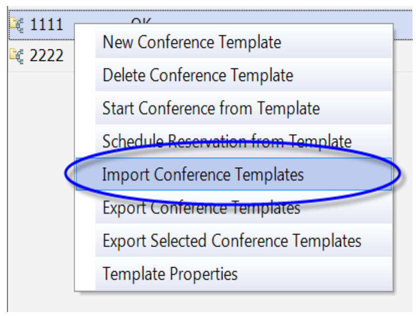
You can import *Conference Templates* and *Conference Profiles* from one MCU to multiple MCUs in your environment.

To import Conference Templates:

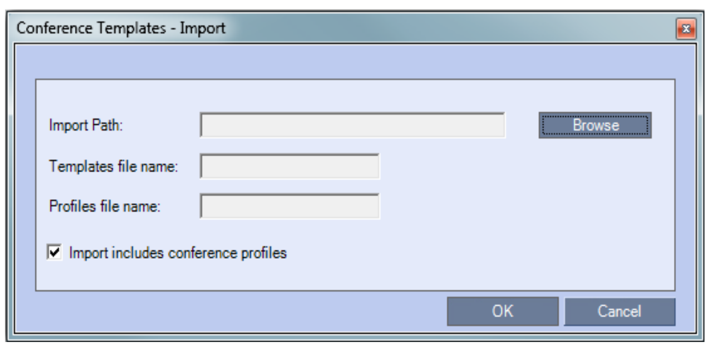
1 In the *RMX Web Client* main window, click the *Conference Templates* tab.

The *Conference Templates* are displayed.

2 Click the **Import Conference Templates**  button or right-click the Conference Templates pane, and then click **Import Conference Templates.**

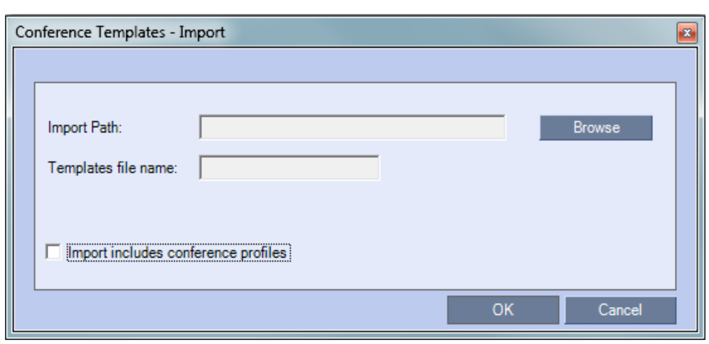


The *Conference Templates - Import* dialog box is displayed.



3 Optional. Clear the **Import includes conference profiles** check box when you only want to import *Conference Templates*.

When this check box is cleared, the *Conference Templates - Import* dialog box is displayed without the *Profiles file name* field.



4 In the *Import Path* field, click **Browse** to navigate to the path and file name of the *Conference Templates* you want to import.

When clicking the exported templates file you want to import, the system automatically displays the appropriate files in the *Templates file name* field and the *Profiles file name* field (when the **Import includes conference profiles** check box is selected).

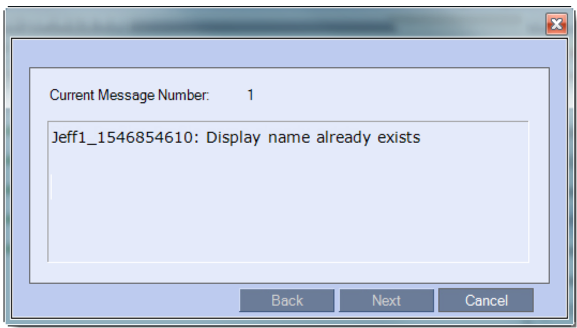
5 Click **OK** to import the *Conference Templates* and their associated *Conference Profiles,* if selected.

Conference Templates are not imported when:

— A *Conference Template* already exists

— An associated *Conference Profile* is not defined in the *Conference Profiles* list

When one or more *Conference Templates* are not imported, a Message Alert window is displayed with the templates that were not imported.



6 Click **Cancel** to exit the *Message Alerts* window.

The imported *Conference Templates* are added to the *Conference Templates* list. When the **Import includes conference profiles** check box is selected, the imported *Conference Profiles* are added to the *Conference Profiles* list.

12

Polycom Conferencing for Microsoft Outlook®

> Polycom Conferencing for Microsoft Outlook is supported in AVC Conferencing Mode only.

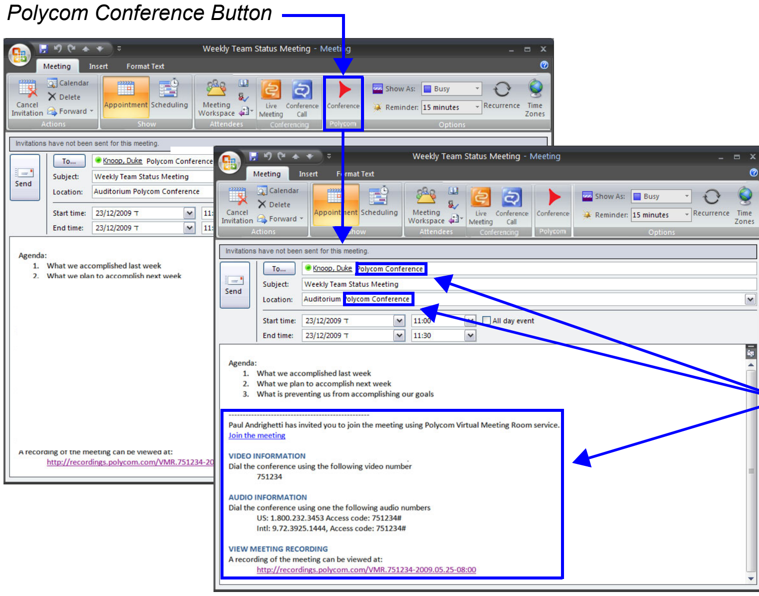
Polycom Conferencing for Microsoft Outlook is an add-in that enables users to easily organize and invite attendees to *Video Enabled* meetings via *Microsoft Outlook*®.

Polycom Conferencing for Microsoft Outlook is implemented by installing the *Polycom Conferencing Add-in for Microsoft Outlook* on *Microsoft Outlook*®
e-mail clients. It enables meetings to be scheduled with video endpoints from within *Outlook*. The add-in also adds a *Polycom Conference* button in the *Meeting* tab of the *Microsoft Outlook* e-mail client ribbon.

The meeting organizer clicks the **Polycom Conference** button to add *Conference Information* to the meeting invitation.

Attendees call the meeting at the scheduled *Start Time* using the link or the dial-in number provided in the meeting invitation.

Polycom Conference Button



Conference Information Added

A *Gathering Slide* is displayed to connected participants until the conference starts.

Gathering Slide: *Displays Meeting Information Until Conference Starts*

The *Gathering Slide* displays live video along with information taken from the meeting invitation such as the subject, meeting organizer, duration, dial-in numbers etc. At the end of the *Gathering Phase*, the conference layout is displayed.

For more information see "*Video Preview"* on page **4-26**.

Setting up the Calendaring Solution

The following steps are performed to set up the Calendaring solution:

A The administrator installs the *Polycom Conferencing Add-in for Microsoft* for *Microsoft Outlook* e-mail clients. For more information, see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

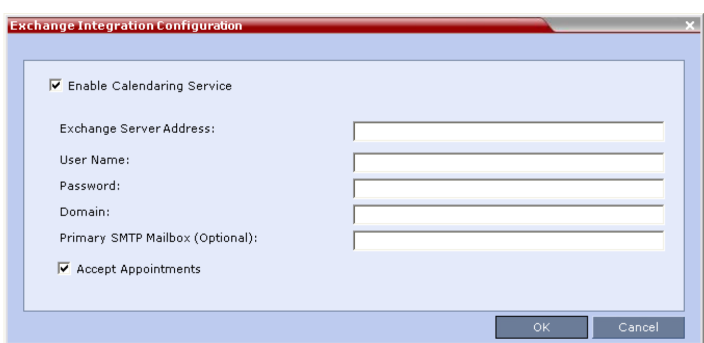
B The administrator creates an *Microsoft Outlook* e-mail-account for the RMX.
If included in the solution, *Polycom DMA system* (*DMA*) and calendaring-enabled endpoints share this e-mail account. For more information, see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

C The administrator configures the RMX for *Calendaring* using the *Exchange Integration Configuration* dialog box, providing it with the *Microsoft* Exchange Server Name, User Name and Password and optional Primary SMTP Mail box information needed to access the
e-mail account.

To configure the RMX's Exchange Integration Configuration:

1 On the RMX menu, click **Setup > Exchange Integration Configuration**.

The *Exchange Integration Configuration* dialog box is displayed.



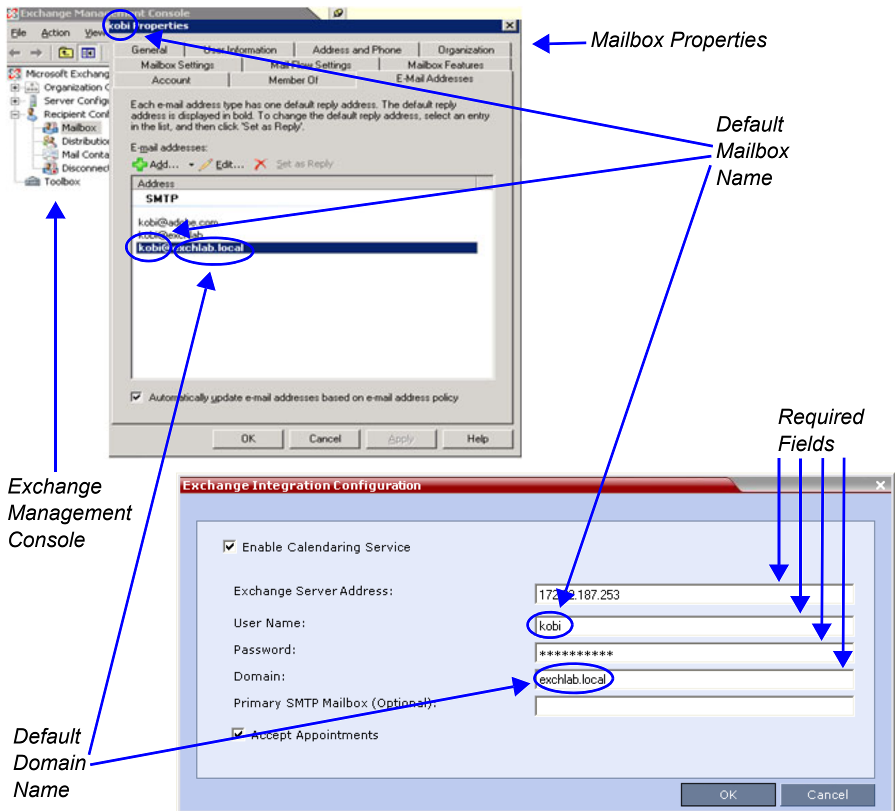
There are three options that can be used to configure the *Exchange Integration Configuration*. The option you choose will depend on the configuration of the mailbox in the *Exchange Server* and the configuration of the *Exchange Server* itself.

— **Option 1** - Use this option if the *Exchange Server* settings have been left at their default values.

— **Option 2** - Use this option if the *Primary SMTP Mailbox* is not the default mailbox.

— **Option 3** - Use this option if the *Exchange Server* settings have been modified by the administrator.

Option 1 - Using default Exchange Server settings



a Define the following fields:

Table 12-1 *Exchange Integration Configuration - Option 1*

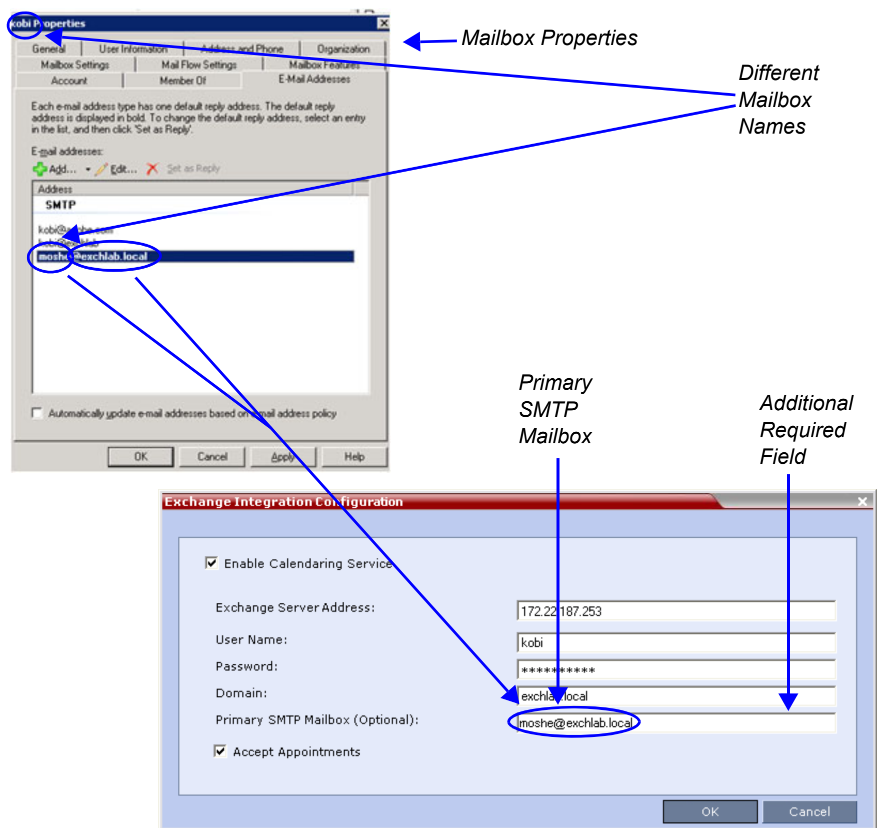
Field	Description
Enable Calendaring Service	Select or clear this check box to enable or disable the Calendaring Service using the Polycom Add-in for Microsoft Outlook. When this check box is cleared all fields in the dialog box are disabled.
Exchange Server Address	Enter the IP address of the Exchange Server.

***Table 12-1** Exchange Integration Configuration - Option 1 (Continued)*

Field	Description
User Name	Enter the User Name of the RMX, as registered in the Microsoft Exchange Server, that the RMX uses to login to its e-mail account. Field length: Up to 80 characters.
Password	Enter the Password the RMX uses to login to its e-mail account as registered in the Microsoft Exchange Server. Field length: Up to 80 characters.
Domain	Enter the name of the network domain where the RMX is installed as defined in the Microsoft Exchange Server.
Primary SMTP Mailbox (Optional)	This field is left empty.
Accept Appointments	Select this check box to enable the RMX to send replies to meeting invitations. Clear this check box when the RMX is part of a Unified Conferencing solution that includes a DMA, as the DMA will send a reply to the meeting invitation.

b Click the **OK** button.

Option 2 - Using an alternate Primary SMTP Mailbox



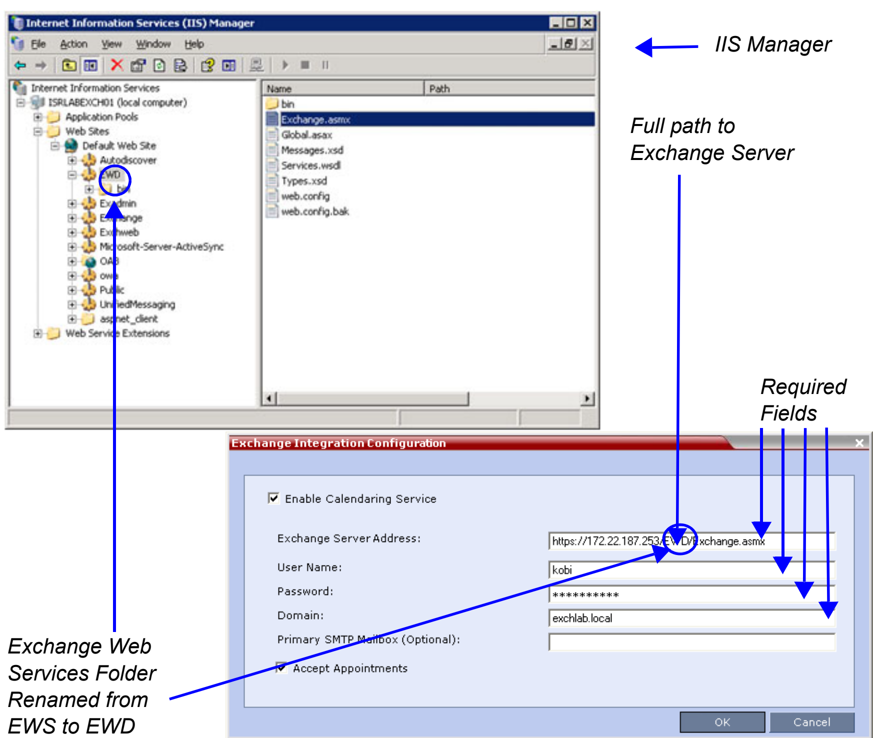
a Define the following fields:

Table 12-2 *Exchange Integration Configuration - Option 2*

Field	Description
Enable Calendaring Service	These fields are defined as for **Option 1** above.
Exchange Server Address	
User Name	
Password	
Domain	
Accept Appointments	
Primary SMTP Mailbox (Optional)	Enter the name of the SMTP Mailbox in the Microsoft Exchange Server to be monitored by the RMX. **Note:** Although several mailboxes can be assigned to each user in the Microsoft Exchange Server, only the Primary SMTP Mailbox is monitored. The Primary SMTP Mailbox name does not have to contain either the RMX's User Name or Domain name.

b Click the **OK** button.

Option 3 - Using modified Exchange Server settings



a Define the following fields:

Table 12-3 Exchange Integration Configuration - Option 3

Field	Description
Exchange Server Address	If Exchange Server settings have been modified, enter the full path to the Microsoft Exchange Server where the RMX's Microsoft Outlook e-mail account is registered, for example if the EWS folder has been renamed *EWD*: `https://labexch01/`**`EWD`**`/Exchange.asmx` **Note:** If a server name is entered, the RMX and the Microsoft Exchange Server must be registered to the same Domain. (The Domain name entered in this dialog box must match the Local Domain Name entry in the Management Network - DNS Properties dialog box.) For more information see "*Modifying the Management Network"* on page **16-3**. Field length: Up to 80 characters.
Enable Calendaring Service	These fields are defined as for **Option 1** above.
User Name	
Password	
Domain	
Primary SMTP Mailbox (Optional)	
Accept Appointments	

b Click the **OK** button.

If applicable, *RSS, VMC*, *DMA* and calendaring-enabled endpoints are configured with the *Exchange Server Name, User Names* and *Passwords* needed to access their accounts.

For more information see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

2 The administrator configures the RMX to have a default *Ad-hoc Entry Queue* service enabled. If *ISDN/PSTN* participants are included, up to two *ISDN/PSTN* dial-in numbers must be configured for the *Ad Hoc Entry Queue*.
For more information see "*Defining a New Entry Queue"* on page **7-3**.

Calendaring Guidelines

- The RMX must have its *MCU* prefix registered in the gatekeeper.
  For more information see "*Modifying the Default IP Network Service"* on page **16-11**.
- The RMX must be configured as a *Static Route*.
  For more information see "*Modifying the Default IP Network Service"* on page **16-11**.
- The RMX's *Default Entry Queue* must be configured as an *Ad Hoc Entry Queue* and must be designated as the *Transit Entry Queue*.
  For more information see the "*Entry Queues"* on page **7-1**.

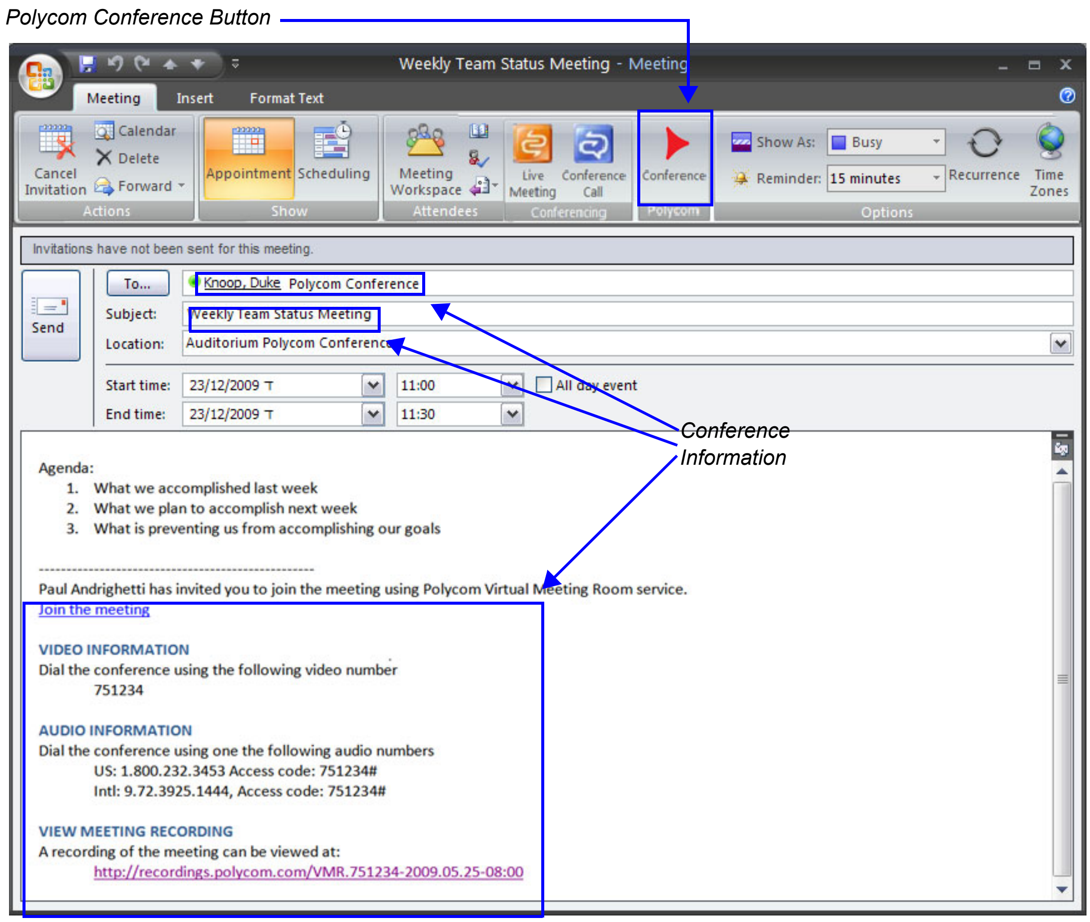
- The meeting organizer can enable recording and/or streaming of the meeting.
- If meeting is to be recorded, the *Ad Hoc Entry Queue* must have recording enabled in its *Profile*.
  For more information see "*Defining New Profiles"* on page **2-18**.
- Meetings can be single instance or have multiple occurrences.
- Attendees that do not have video devices may be invited to the meeting.
- Attendees using e-mail applications that use the *iCalendar* format may be invited to meetings via the *Calendaring Service*.
- Meeting invitations sent by *Polycom Conferencing for Microsoft Outlook* can be in a different language to the *RMX Web Client*. The following languages are supported:
  - English
  - French
  - German
  - International Spanish
  - Korean
  - Japanese
  - Simplified Chinese
- RMX resource management is the responsibility of the system administrator:
  - Conferences initiated by Polycom Conferencing for Microsoft Outlook are ad hoc and therefore resources are not reserved in advance.
  - Polycom Conferencing for Microsoft Outlook Add-in assumes that sufficient resources are available and does not check resource availability. Sufficient resources are therefore not guaranteed.
  - A meeting invitation that is automatically accepted by the RMX is not guaranteed availability of resources.
  - If the RMX runs out of resources, attendees will not be able to connect to their conferences.
- By using DMA to load-balance resources between several RMXs, resource capacity can be increased, alleviating resource availability problems.

Creating and Connecting to a Conference

Creating a Conference

Meetings are organized using the *Microsoft Outlook* client in the normal manner.

If the meeting organizer decides that video participants are to be included in a multipoint video conference, he/she clicks the **Polycom Conference** button. *Conference Information* such as the *Meeting ID* and connection information is automatically added to the existing appointment information.



The meeting organizer can add a meeting agenda or personal text to the invitation before it is sent. The meeting organizer can update or cancel the video enabled meeting in the same manner as for any other meeting.

When the meeting organizer sends the meeting invitation a meeting record is saved in the *Microsoft Exchange Server*, the RMX, *DMA, RSS* and calendaring-enabled endpoints.

RMXs, *DMA* and calendaring-enabled endpoints poll the *Microsoft Exchange Server* to retrieve new meeting records and updates to existing meeting records.

Table 12-4 summarizes the RMX's usage of *Microsoft Outlook* data fields included in the meeting invitation.

Table 12-4 *Microsoft Outlook Field Usage*

Microsoft Outlook Field	Usage by the RMX / DMA	
	Conference / Meeting Room	**Gathering Slide**
Subject	Display Name of Conference / Meeting Room.	Meeting Name.
Start/End Time	Used to calculate the Conference's Duration.	
Record	Enable Recording in the Conference or Meeting Room Profile.	Display Recording option.
Video Access Number	Comprised of: `<MCU Prefix in Gatekeeper> <Conference Numeric ID>`. **Note:** It is important that *MCU Prefix in Gatekeeper* field in the RMX's *IP Network Service - Gatekeeper* tab and the *Dial-in prefix* field in the *Polycom Conferencing Add-in for Microsoft Outlook - Video Network* tab contain the same prefix information.	Displayed as the IP dial in number in the Access Number section of the Gathering Slide.
Video Access Number (Cont.)	If Recording and Streaming are enabled in the Conference Profile, this number is used as part of the recording file name.	
Audio Access Number	ISDN/PSTN dial-in number. Up to two numbers are supported.	Displayed as the ISDN/PSTN dial-in number in the Access Number section of the Gathering Slide.
Streaming recording link	Enables the recording of the conference to the Polycom RSS using the recording link. Enables streaming of the recording of the conference from the Polycom RSS.	If recording is enabled, a REC indicator is displayed in the top left corner of the slide.

Connecting to a Conference

Participants can connect to the conference in the following ways:

- Participants with *Polycom CMA Desktop™* or a *Microsoft Office Communicator* client running on their PCs can click on a link in the meeting invitation to connect to the meeting.
- Participants with a *HDX* or a room system will receive a prompt from the endpoint's calendaring system along with a button that can be clicked in order to connect. Participants with endpoints that are not calendaring-enabled can connect to the meeting by dialing the meeting number manually.

- Participants outside the office or using *PSTN* or mobile phones, can use the dial in number in the meeting invitation to manually dial in to the meeting.

RMX Standalone Deployment

When using a single RMX in a standalone deployment, connection is via an *Ad Hoc Entry Queue*. The meeting is started when the first participant connects to the RMX.

When the first participant connects, a conference is created and named according to the information contained in the dial string. Subsequent participants connecting with the same dial string are routed from the *Ad Hoc Entry Queue* to the conference.

After the conference has been created the *Conference Name, Organizer, Time, Duration* and *Password* (if enabled) are retrieved from the conference parameters for display during the *Gathering Phase*.

RMX and Polycom DMA System Deployment

In a *DMA* deployment a *Virtual Meeting Room* is activated when the first participant connects to the *DMA*. *DMA* receives the dial string to activate a *Virtual Meeting Room* on the RMX.

DMA uses the *Meeting ID* contained in the dial-in string to access meeting information stored in the *Exchange Server* database.

When the meeting information is found on the *Exchange Server*, the *Conference Name, Organizer, Time, Duration* and *Password* (if enabled) are retrieved from the *Exchange Server* database for display during the *Gathering Phase*.

> If enabled, automatically generated passwords are ignored.
> For more information see "*Automatic Password Generation Flags*" on page **22-45**.

Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners. These additional services will help customers successfully design, deploy, optimize and manage Polycom visual communications within their UC environments.

Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. For additional information and details please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

13

Conference and Participant Monitoring

Viewing Permissions			
Tab	Chairperson	Operator	Administrator
Skins	✔	✔	✔
IVR		✔	✔
Info	✔	✔	✔

You can monitor ongoing conferences and perform various operations while conferences are running.

Three levels of monitoring are available with the RealPresence Collaboration Server (RMX):

- *General Monitoring* - You can monitor the general status of all ongoing conferences and their participants in the main window.
- *Conference Level Monitoring* - You can view additional information regarding a specific conference and modify its parameters if required, using the *Conference Properties* option.
- *Participant Level Monitoring* - You can view detailed information on the participant's status, using the *Participant Properties* option.
- The maximum number of participants:

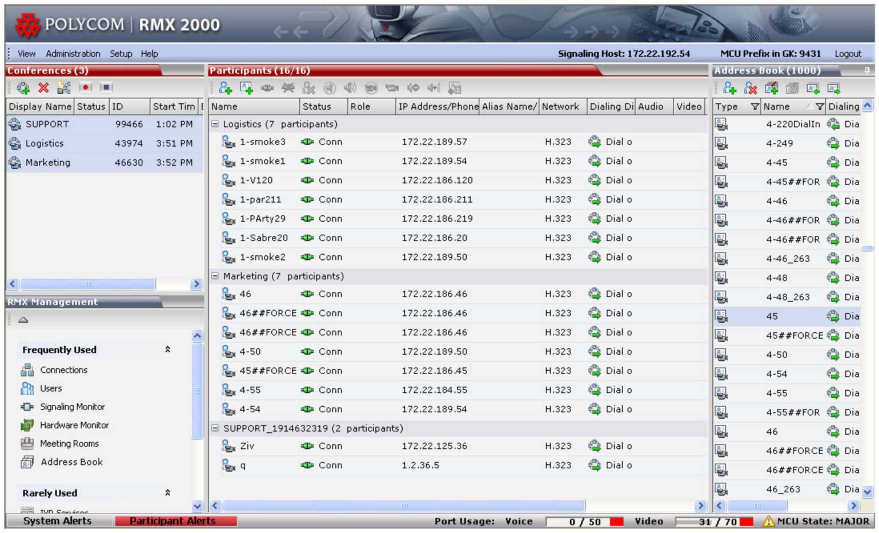
The following numbers are for *MPM* card assemblies with maximum resource capacities.

— RealPresence Collaboration Server (RMX) 1500 *MPMx Mode*: 360 (90 video).
— RealPresence Collaboration Server (RMX) 2000 *MPM Mode*: 400 (80 video).
— RealPresence Collaboration Server (RMX) 2000 *MPM+ Mode*: 800 (160 video).
— RealPresence Collaboration Server (RMX) 2000 *MPMx Mode*: 720 (180 video).
— RealPresence Collaboration Server (RMX) 4000 *MPM+ Mode*: 1600 (160 video).
— RealPresence Collaboration Server (RMX) 4000 *MPMx Mode*: 1440 (180 video).

From *Version 7.1*, *MPM* media cards are not supported.

General Monitoring

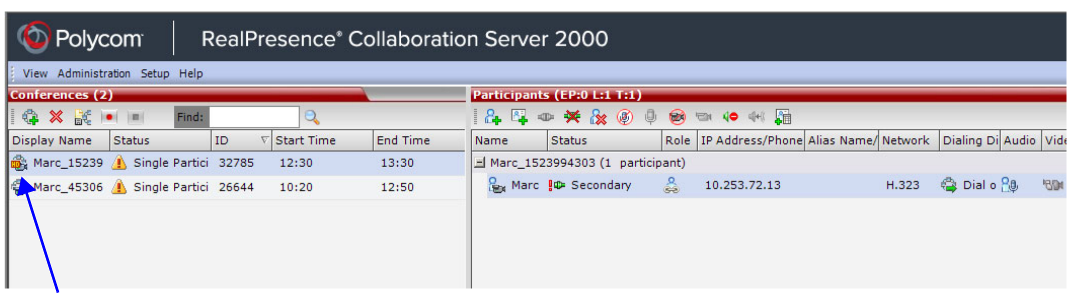
Users can monitor a conference or keep track of its participants and progress. For more information, see *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Monitoring Ongoing Conferences"* on page **3-39**.



You can click the blinking **Participant Alerts** indication bar to view participants that require attention. For more information, see "*System and Participant Alerts"* on page **21-1**.

Monitoring AVC-based Video Switching Conferences

Video Switching conferences appear with the HD () icon in the conferences list to differentiate between CP and VSW conferences.



HD Conference

Monitoring is done in the same way as for CP conferences.

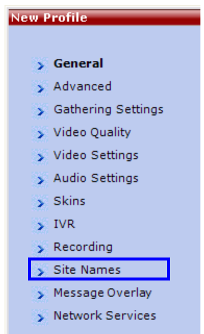
Conference Level Monitoring

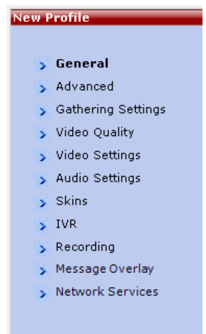
In addition to the general conference information that is displayed in the *Conference* list pane, you can view the details of the conference's current status and setup parameters, using the *Conference Properties* dialog box.

The tabs displayed in the *Conference Properties* dialog boxes are dependent on the *Conferencing Mode* and the *Card Configuration Mode* of the RMX—whether the RMX is configured with *MPMx* or *MPM+* cards.

Viewing the Properties of an Ongoing AVC-based Conference

In *MPMx Mode*, *Site Names* is displayed as an additional tab and dialog box whereas in *MPM+ Mode*, *Site Names* is a selection within the *Video Settings* dialog box.



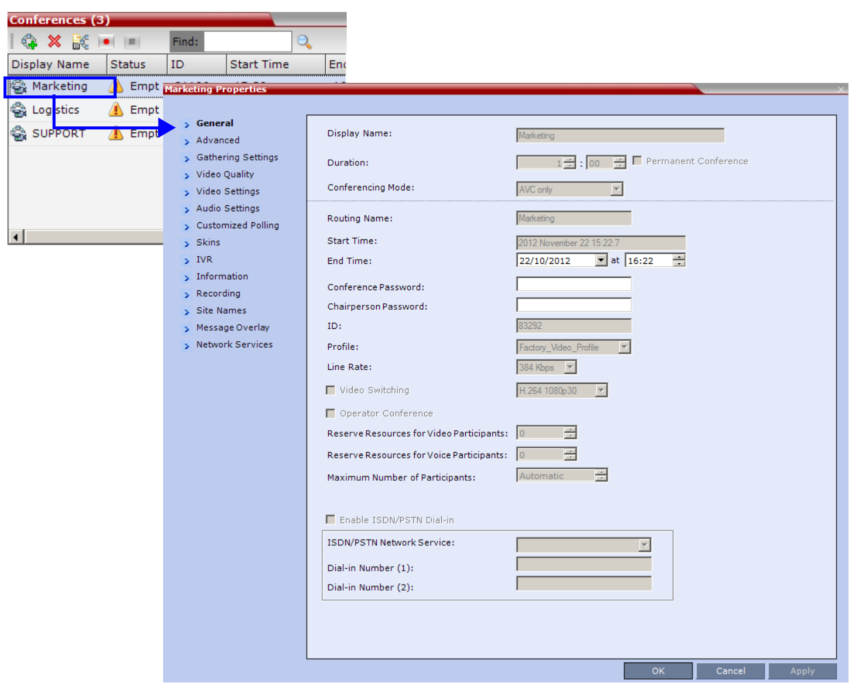


To view the parameters of an ongoing AVC conference:

1 In the *Conference* list pane, double-click the AVC conference or right-click the AVC conference and then click **Conference Properties**.

The *Conference Properties - General* dialog box with the **General** tab opens.

Viewing Permissions			
Tab	Chairperson	Operator	Administrator
General	✔	✔	✔



The following information is displayed in the *General* tab:

***Table 13-1** Conference Properties - General*

Field	Description
Display Name	The Display Name is the conference name in native language and Unicode character sets to be displayed in the *RealPresence Collaboration Server Web Client*. **Note:** This field is displayed in all tabs.
Duration	The expected duration of the conference using the format HH:MM. **Note:** This field is displayed in all tabs.
Routing Name	The ASCII name of the conference. It can be used by H.323 and SIP participants for dialing in directly to the conference. It is used to register the conference in the gatekeeper and the SIP server.
Conferencing Mode	The conferencing mode for the conference.
Start Time	The time the conference started.
End Time	The expected conference end time.
Conference Password	A numeric password for participants to access the conference.
Chairperson Password	A numeric password used by participants to identify themselves as the conference chairperson.
ID	The conference ID.
Profile	The name of the conference Profile from which conference parameters were taken.
Line Rate	The maximum transfer rate, in kilobytes per second (Kbps) of the call (video and audio streams).

Table 13-1 *Conference Properties - General (Continued)*

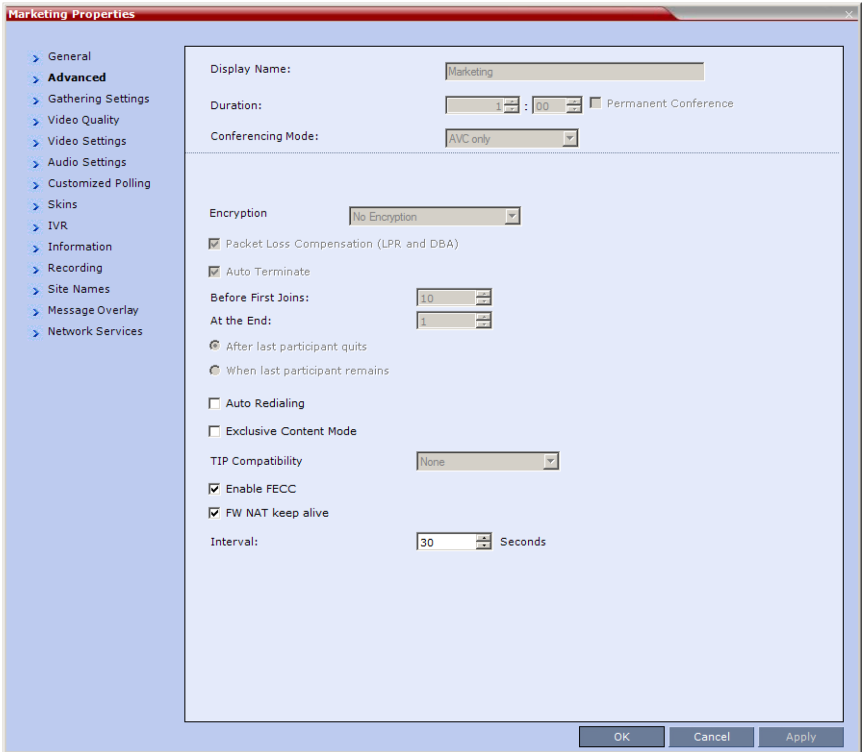
Field	Description

Video Switching	When selected, the conference is of ultra-high quality video resolution, in a special conferencing mode which implies that all participants must connect at the same line rate and use HD video.
	This feature utilizes the resources more wisely and efficiently by:
	• Saving utilization of video ports (1 port per participant as opposed to 4 ports in CP mode).
	• Video display is in full screen mode only.
	Drawbacks of this feature are that all participants must connect at the same line rate, (e.g. HD) and all participants with endpoints not supporting HD will connect as secondary (audio only).
	Video layout changes are not enabled during a conference.
	Video Switching supports the following resolutions:
	• MPM:
	  • HD 720P
	• MPM+:
	  • HD 1080p
	• MPMx:
	  • 1080p60
	  • 720p30
	  • 720p60
	  • SD30
	If HD 1080p is selected, endpoints that do not support HD 1080p resolution are connected as Secondary (Audio Only) participants.
	Note: Video Switching conferencing mode is unavailable to ISDN participants.
	For more information, see "*Video Resolutions in AVC-based CP Conferencing"* on page **3-1**.

Reserve Resources for Video Participants	Displays the number of video participants for which the system reserved resources. Default: 0 participants.
Reserve Resources for Audio Participants	Displays the number of audio participants for which the system reserved resources. Default: 0 participants.
Max Number of Participants	Indicates the total number of participants that can be connected to the conference. The Automatic setting indicates the maximum number of participants that can be connected to the MCU according to resource availability.
Enable ISDN/PSTN Network Service	When selected, ISDN/PSTN participants can dial into the conference.
ISDN/PSTN Network Service	When the *Enable ISDN/PSTN Network Service* is selected, displays the default Network Service.
Dial-in Number (1)	Displays the conference dial in number.
Dial-in Number (2)	Displays the conference dial in number.

2 Click the **Advanced** tab.

The *Conference Properties - Advanced* dialog box opens.



3 The following information is displayed in the *Advanced* tab:

Table 13-2 *Conference Properties - Advanced Parameters*

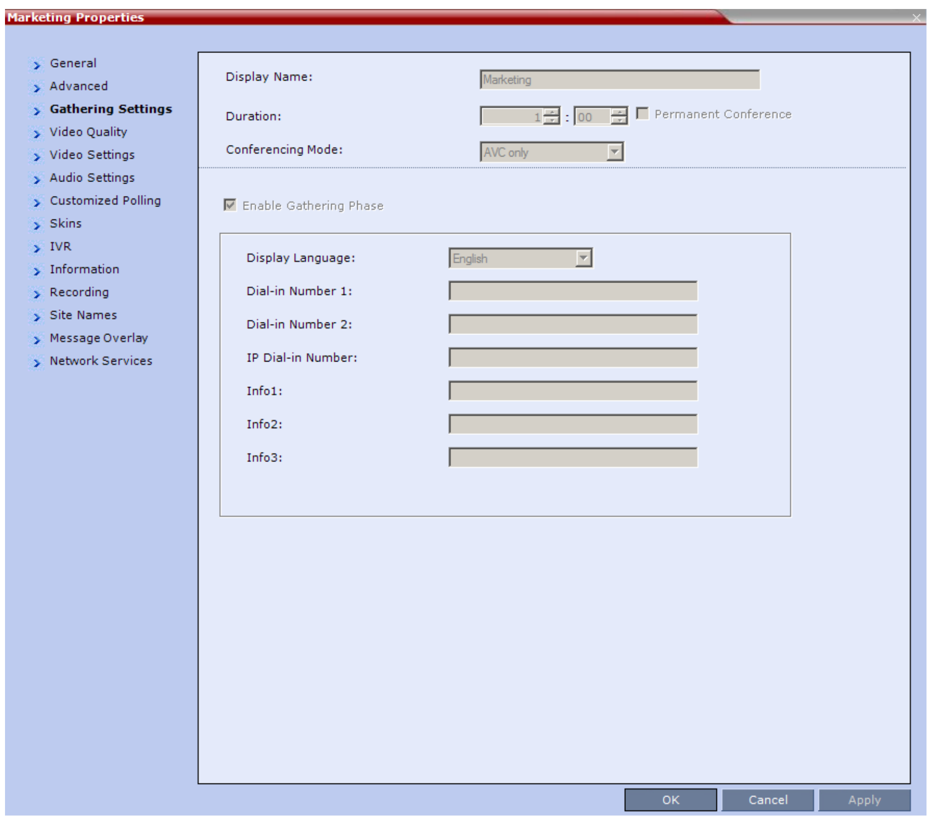
Field/Option	Description
Encryption	Indicates whether the conference is encrypted.
Packet Loss Compensation (LPR and DBA)	Indicates whether Packet Loss Compensation is enabled.
Auto Terminate	When selected, indicates that the MCU will automatically terminate the conference when *Before First Joins*, *At the End-After Last Quits and At the End - When Last Participant Remains* parameters apply.
Auto Redialing	Indicates whether dial-out participants are automatically (when selected) or manually (when cleared) connected to the conference.
Exclusive Content Mode	When selected, *Content* is limited to one participant.

***Table 13-2** Conference Properties - Advanced Parameters (Continued)*

Field/Option	Description
TIP Compatibility	Indicates the *TIP Compatibility* mode when implementing an *RMX and Cisco Telepresence Systems (CTS) Integration* solution. • None • Video Only • Video & Content The *TIP Compatibility* mode affects in the user video and content experience. For more information, see "*Collaboration With Cisco's Telepresence Interoperability Protocol (TIP)"* on page **I-1**.
Enable FECC	When selected, Far End Camera Control is enabled.
FW NAT Keep Alive	When selected, sends a *FW NAT Keep Alive* message at specific Intervals for the RTP, UDP and BFCP channels. The interval specifies how often a *FW NAT Keep Alive* message is sent. For more information, see "*NAT (Network Address Translation) Traversal"* on page **16-72**

4 Click the **Gathering Settings** tab.

The *Conference Properties - Gathering Settings* dialog box opens.



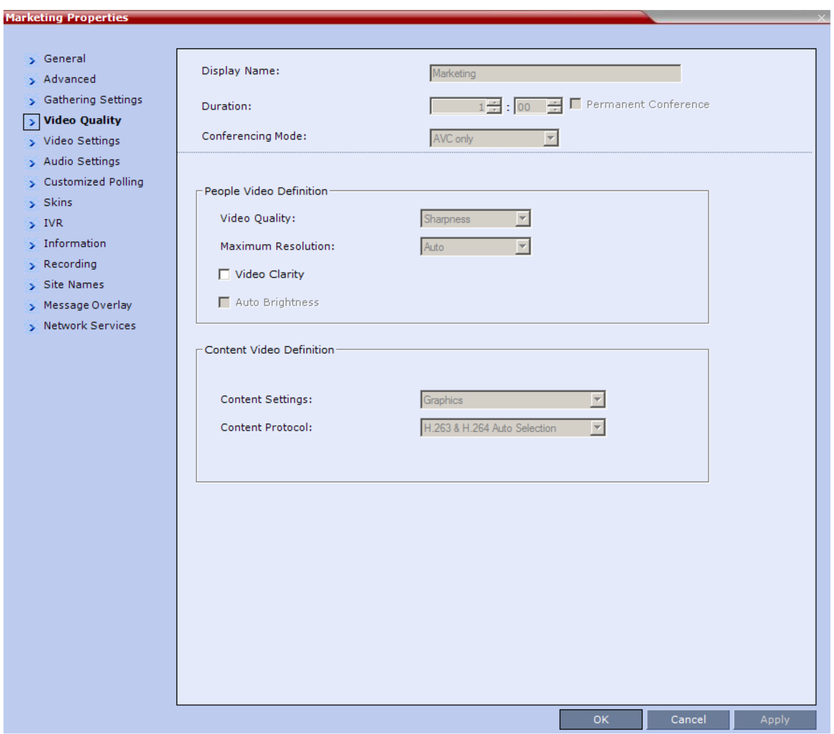
5 The following information is displayed:

Table 13-3 *Profile - Gathering Settings*

Field/Options	Description
Enable Gathering	Indicates whether the *Gathering Phase* has been enabled.
Display Language	Indicates the language of the *Gathering Slide* field headings. **Note:** When working with the *Polycom Conferencing Add-in for Microsoft Outlook,* the language selected should match the language selected for the conference in the *Polycom Conferencing Add-in for Microsoft Outlook* to ensure that the *Gathering Phase* slide displays correctly.
Access Number 1	Indicates the ISDN or PSTN number(s) to call to connect to the conference. Note: The numbers entered must be verified as the actual Access Numbers.
Access Number 2	
Info 1	Additional information to be displayed during the *Gathering Phase*.
Info 2	
Info 3	

6 Click the **Video Quality** tab.

The *Conference Properties - Video Quality* dialog box opens.



The following information is displayed:

Table 13-4 *Conference Properties - Video Quality Parameters*

Field/Option	Description
People Video Definition	
Video Quality	Indicates the resolution and frame rate that determine the video quality set for the conference. Possible settings are: **Motion** or **Sharpness**. For more information, see *"Video Resolutions in AVC-based CP Conferencing"* on page **3-1**.
Maximum Resolution	This setting overrides the *Maximum Resolution* setting of the *Resolution Configuration* dialog box. The administrator can select one of the following *Maximum Resolution* options: • *Auto* (default) - The *Maximum Resolution* remains as selected in the *Resolution Configuration* dialog box. • *CIF* • *SD* • *HD720* • *HD1080* *Maximum Resolution* settings can be monitored in the *Profile Properties - Video Quality* and *Participant Properties - Advanced* dialog boxes. **Notes:** The *Resolution* field in the *New Participant - Advanced* dialog box allows *Maximum Resolution* to be **further limited** per participant endpoint. The *Maximum Resolution* settings for conferences and participants cannot be changed during an ongoing conference.
Video Clarity™	Indicated if Video Clarity is enabled for the conference.
Auto Brightness	*Auto Brightness* detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout. • *Auto Brightness* is supported with MPM+ and MPMx cards only. • *Auto Brightness* only increases brightness and does not darken video windows. • *Auto Brightness* is selected by default. • *Auto Brightness* cannot be selected and deselected during an ongoing conference. **Default**: On **Note:** When *Auto Brightness* is enabled, color changes may be observed in computer-based *VGA Content* sent by *HDX* endpoints through the *People* video channel.

Table 13-4 *Conference Properties - Video Quality Parameters (Continued)*

Field/Option	Description
Content Video Definition	
Content Settings	Indicates the Content channel resolution set for the conference. Possible resolutions are: • **Graphics –** default mode • **Hi-res Graphics –** requiring a higher bit rate • **Live Video –** content channel is live video • **Customized Content Rate** - resolution is manually defined.

Content Protocol	• **H.263**
	  • *Content* is shared using the *H.263* protocol.
	  • Use this option when most of the endpoints support *H.263* and some endpoints support *H.264*.
	• **H.263 & H.264 Auto Selection** (Default)
	  • *Content* is shared using *H.263* if a mix of H.263-supporting and *H.264*-supporting endpoints are connected.
	  • *Content* is shared using *H.264* if all connected endpoints have *H.264* capability.
	• **H.264 Cascade Optimized and SVC Optimized**
	  • All *Content* is shared using the *H.264* content protocol and is optimized for use in *Cascaded Conferences*.
	• **H.264 HD**
	  • Ensures high quality *Content* when most endpoints support *H.264* and *HD Resolutions*.

7 Click the **Video Settings** tab to list the video parameters.

Viewing Permissions			
Tab	*Chairperson*	*Operator*	*Administrator*
Video Settings	✔	✔	✔

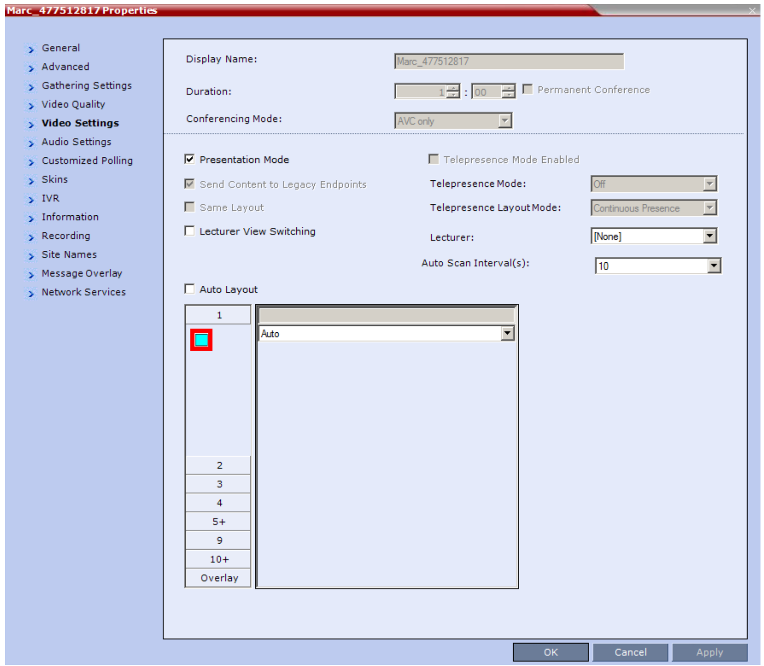


***Table 13-5** Conference Properties - Video Settings Parameters*

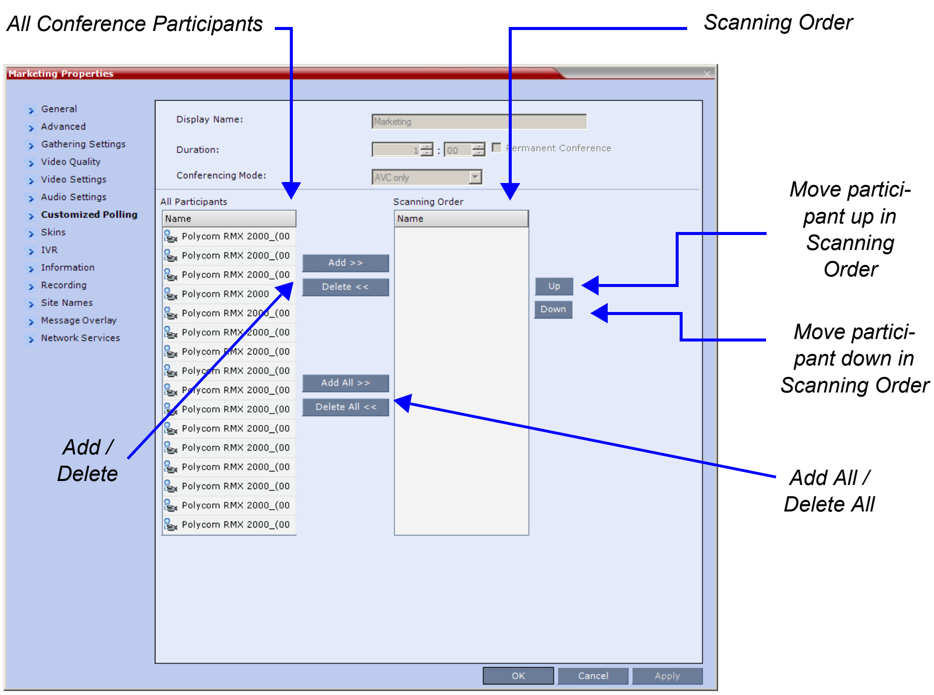
<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>Presentation Mode</td><td colspan="2">When checked, indicates that the Presentations Mode is active. For more information, see "Presentation Mode” on page 2-30.</td></tr>
<tr><td>Lecturer View Switching</td><td colspan="2">When checked, the Lecturer View Switching enables automatic random switching between the conference participants in the lecturer video window.</td></tr>
<tr><td>Same Layout</td><td colspan="2">When checked, forces the selected layout on all conference participants, and the Personal Layout option is disabled.</td></tr>
<tr><td>Send Content to Legacy Endpoints</td><td colspan="2">Select this option to enable Legacy endpoints to send content to H.323/SIP/ISDN endpoints that do not support H.239 Content (legacy endpoints) over the video (people) channel, allowing all conference participants to view the content.</td></tr>
<tr><td>Auto Layout</td><td colspan="2">When enabled, the system automatically selects the conference layout based on the number of participants in the conference.</td></tr>
<tr><td>Telepresence Mode Enabled</td><td>Indicates if the conference is running in Telepresence Mode.</td><td rowspan="3">These fields are enabled if the RMX has a Telepresence license installed.
See "Defining New Profiles” on page 2-18.</td></tr>
<tr><td>Telepresence Mode</td><td>Indicates the Telepresence Mode.</td></tr>
<tr><td>Telepresence Layout Mode</td><td>Indicates the layout of the Telepresence Mode.</td></tr>
<tr><td>Lecturer</td><td colspan="2">Indicates the name of the lecturer (if one is selected). Selecting a lecturer enables the Lecture Mode.</td></tr>
</table>

Table 13-5 *Conference Properties - Video Settings Parameters (Continued)*

Field	Description
Auto Scan Interval(s)	The time interval, 10 - 300 seconds, that Auto Scan uses to cycle the display of participants that are not in the conference layout in the selected cell.
Video Layouts (graphic)	Indicates the currently selected video layout.

8 Click the **Audio Settings** tab to view the audio setting for the conference. You can modify the *Mute participants except lecturer* setting.

9 Click the **Customized Polling** tab to view and modify the customized polling for the conference.



All conference participants are listed in the left pane (*All Participants*) while the participants that are to be displayed in the Auto Scan enabled cell of the video layout are listed in the right pane (*Scanning Order*).

The dialog box buttons are summarized in Table 13-6.

Table 13-6 *Customized Polling - Buttons*

Button	Description
Add	Select a participant and click this button to *Add* a the participant to the list of participants to be Auto Scanned. The participants name is removed from the *All Participants* pane.
Delete	Select a participant and click this button to *Delete* the participant from the list of participants to be *Auto Scanned*. The participants name is moved back to the *All Participants* pane.

Table 13-6 *Customized Polling - Buttons*

Button	Description
Add All	Add all participants to the list of participants to be *Auto Scanned*. All participants' names are removed from the *All Participants* pane.
Delete All	Delete all participant from the list of participants to be *Auto Scanned*. All participants' names are moved back to the *All Participants* pane.
Up	Select a participant and click this button to move the participant *Up* in the *Scanning Order*.
Down	Select a participant and click this button to move the participant *Down* in the *Scanning Order*.

10 **Optional.** Add a participant to the list of participants to be *Auto Scanned*:

- a Click on the participant's name in the *All Participants* list.
- b Click the **Add** button to move the participant to the *Scanning Order* pane.

11 **Optional.** Delete a participant from the list of participants to be *Auto Scanned*:

- a Click on a participant's name in the *Scanning Order* list.
- b Click the **Delete** button to move the participant back to the *All Participants* pane.

12 **Optional.** Add all participants to the list of participants to be *Auto Scanned*:

— Click the **Add All** button.

13 **Optional.** Delete all participant from the list of participants to be *Auto Scanned*:

— Click the **Delete All** button.

14 **Optional.** Move the participant up in the *Scanning Order*:

— Click the **Up** button.

15 **Optional.** Move the participant down in the *Scanning Order*:

— Click the **Down** button.

16 Click the **Apply** button to confirm and keep the *Conference Properties* dialog box open.

or

Click the **OK** the button to confirm and return to the *RealPresence Collaboration Server Web Client Main Screen*.

17 Click the **Skins** tab to view the skin selected for the conference.

You cannot select another skin during an ongoing conference.

18 Click the **IVR** tab to view the IVR settings.

19 Click the **Information** tab to view general information defined for the conference. Changes made to this information once the conference is running are not saved to the CDR.

20 Click the **Recording** tab to review the recording settings for the conference.

21 Click **OK** to close the *Conference Properties* dialog box.

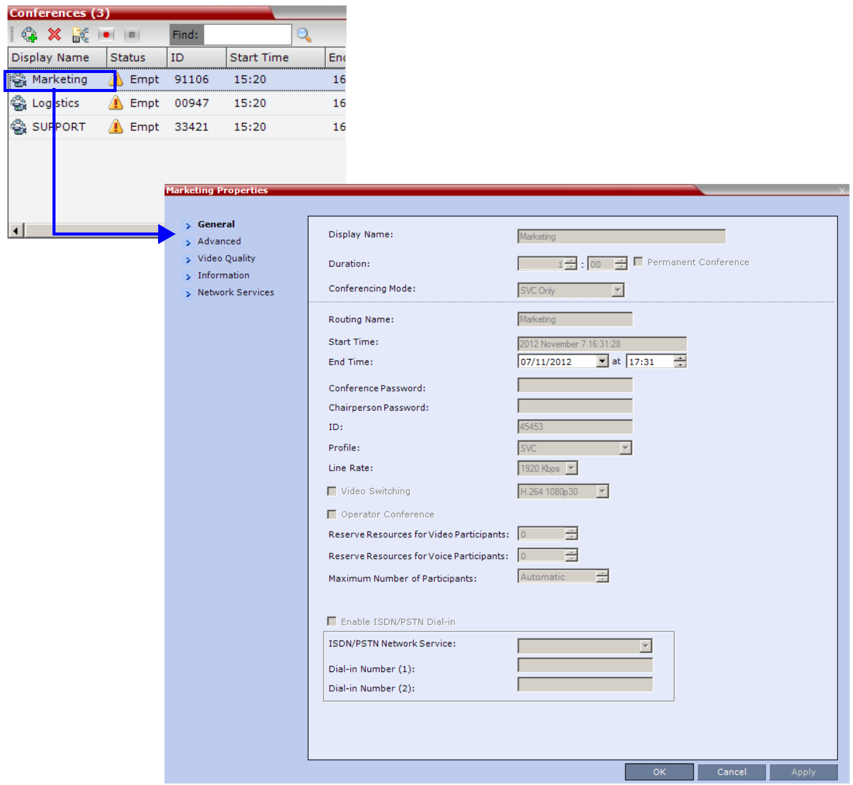
Viewing the Properties of an Ongoing SVC-based Conference

To view the parameters of an ongoing SVC conference:

1 In the *Conference* list pane, double-click the SVC conference or right-click the SVC conference and then click **Conference Properties**.

The *Conference Properties - General* dialog box with the **General** tab opens.

Viewing Permissions			
Tab	Chairperson	Operator	Administrator
General	✔	✔	✔



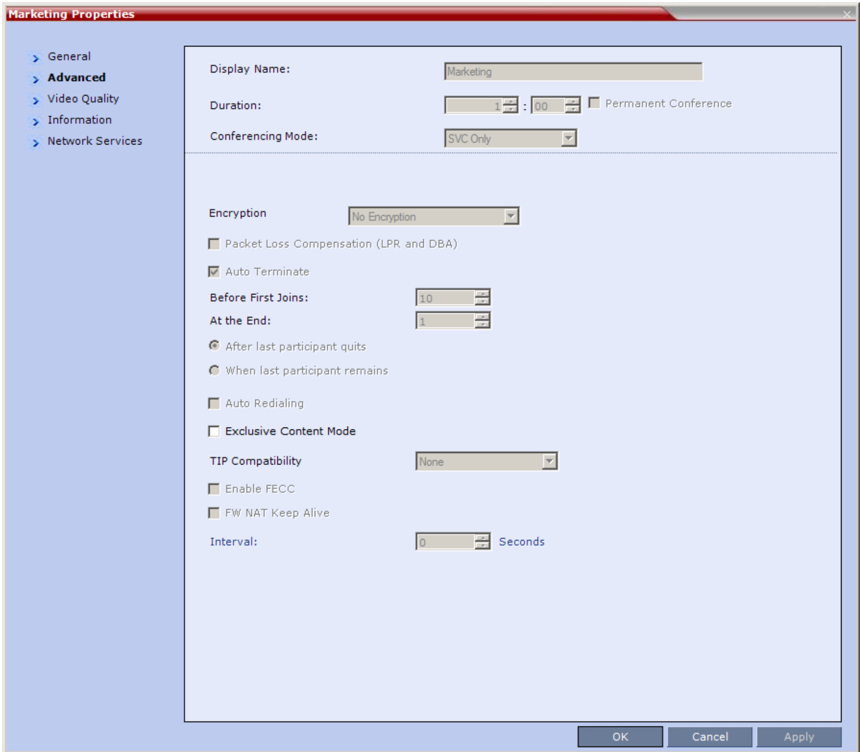
2 The following information is displayed in the *General* tab:

Field	Description
Display Name	The Display Name is the conference name in native language and Unicode character sets to be displayed in the *RealPresence Collaboration Server Web Client*. **Note:** This field is displayed in all tabs.
Duration	The expected duration of the conference using the format HH:MM. **Note:** This field is displayed in all tabs.
Conferencing Mode	The conferencing mode for the conference.
Routing Name	The ASCII name of the conference. It can be used by H.323 and SIP participants for dialing in directly to the conference. It is used to register the conference in the gatekeeper and the SIP server.
Start Time	The time the conference started.
End Time	The expected conference end time.

Field	Description
Conference Password	Conference Password is not supported in SVC conferences.
Chairperson Password	Chairperson Password is not supported in SVC conferences.
ID	The conference ID.
Profile	The name of the conference Profile from which conference parameters were taken.
Line Rate	The maximum transfer rate, in kilobytes per second (Kbps) of the call (video and audio streams).
Video Switching	Video Switching is not supported in SVC conferences.
Reserve Resources for Video Participants	Reserve Resources for Video Participants is not supported in SVC conferences.
Reserve Resources for Audio Participants	Reserve Resources for Audio Participants is not supported in SVC conferences.
Max Number of Participants	Indicates the total number of participants that can be connected to the conference. The Automatic setting indicates the maximum number of participants that can be connected to the MCU according to resource availability.
Enable ISDN/PSTN Network Service	ISDN/PSTN participants are not supported in SVC conferences.
ISDN/PSTN Network Service	ISDN/PSTN participants are not supported in SVC conferences.
Dial-in Number (1)	ISDN/PSTN participants are not supported in SVC conferences.
Dial-in Number (2)	ISDN/PSTN participants are not supported in SVC conferences.

3 Click the **Advanced** tab.

The *Conference Properties - Advanced* dialog box opens.



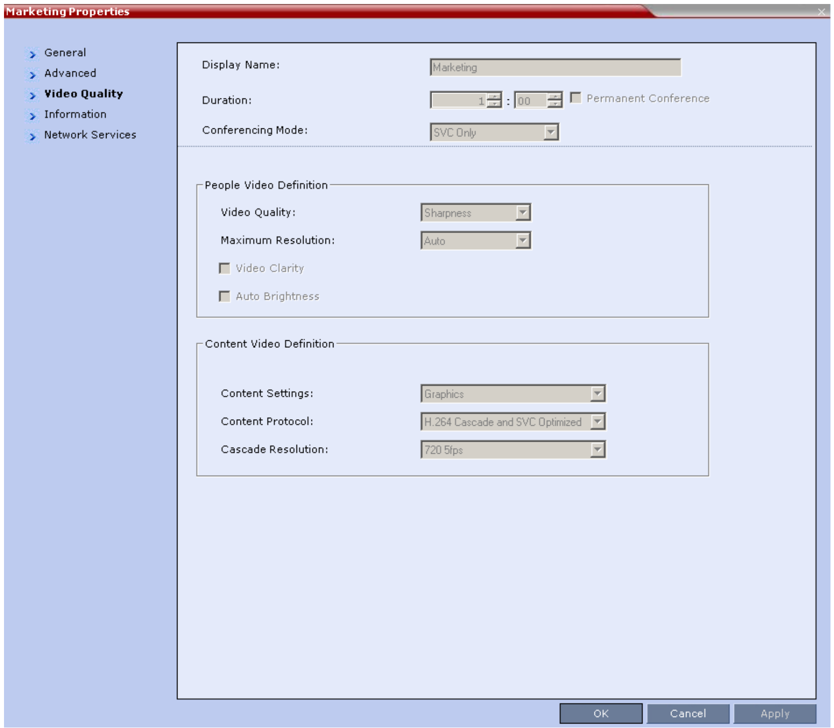
4 The following information is displayed in the *Advanced* tab:

Table 13-7 *Conference Properties - Advanced Parameters*

Field/Option	Description
Encryption	Encryption is not supported in SVC conferences.
Packet Loss Compensation (LPR and DBA)	Packet Loss Compensation is not supported in SVC conferences.
Auto Terminate	When selected, indicates that the MCU will automatically terminate the conference when *Before First Joins*, *At the End-After Last Quits and At the End - When Last Participant Remains* parameters apply.
Auto Redialing	Dial-out is not supported in SVC conferences.
Exclusive Content Mode	When selected, *Content* is limited to one participant.
TIP Compatibility	TIP Compatibility is not supported in SVC conferences.
Enable FECC	Far End Camera Control is not supported in SVC conferences.

5 Click the **Video Quality** tab.

The *Conference Properties - Video Quality* dialog box opens.



The following information is displayed:

Table 13-8 *Conference Properties - Video Quality Parameters*

Field/Option	Description
People Video Definition	
Video Quality	Indicates the resolution and frame rate that determine the video quality set for the conference. In *SVC conferencing*, only Sharpness is supported.
Maximum Resolution	In *SVC conferencing*, this is always *Auto* (default) - The *Maximum Resolution* remains as selected in the *Resolution Configuration* dialog box.
Video Clarity™	Video Clarity is not supported in SVC conferences.
Auto Brightness	*Auto Brightness* is not supported in SVC conferences.
Content Video Definition	
Content Settings	In *SVC conferencing*, this is always set to **Graphics**
Content Protocol	In *SVC conferencing* this is always set to **H.264 Cascade and SVC Optimized**.
Cascade Resolution	Resolution is fixed in SVC conferences.

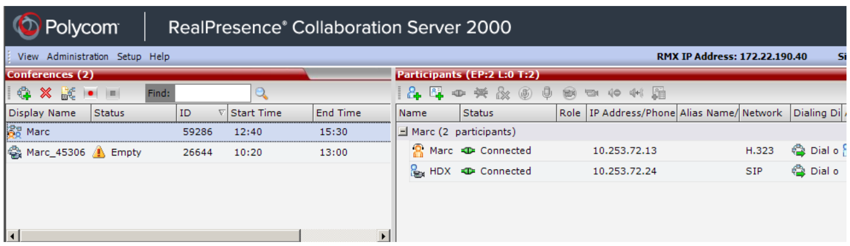
6 Click the **Information** tab to view general information defined for the conference. Changes made to this information once the conference is running are not saved to the CDR.

7 Click **OK** to close the *Conference Properties* dialog box.

Monitoring Operator Conferences and Participants Requiring Assistance

Operator conferences are monitored in the same way as standard ongoing conferences.

Each Operator conference includes at least one participant - the Operator.



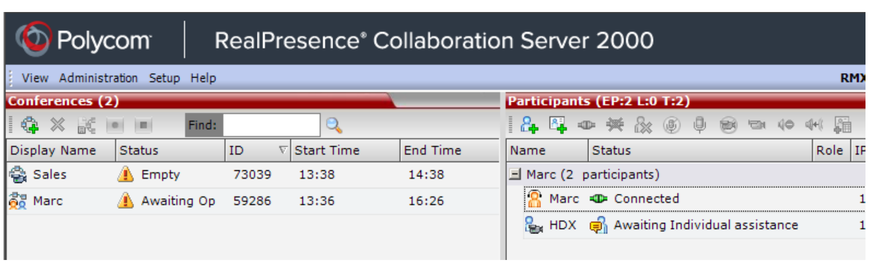
You can view the properties of the *Operator conference* by double-clicking the conference entry in the *Conferences* list or by right-clicking the conference entry and selecting **Conference Properties**. For more information, see the *RealPresence Collaboration Server 1500/ 2000/4000 Getting Started Guide*, "*Conference Level Monitoring*" on page **3-41**.

Requesting Help

A participant can request help using the appropriate DTMF code from his/her touch tone telephone or the endpoint's DTMF input device. The participant can request *Individual Assistance* (default DTMF code ***0**) or *Conference Assistance* (default DTMF code **00**).

Participants in Entry Queues who failed to enter the correct destination conference ID or the conference password will wait for operator assistance (provided that an Operator conference is active).

When requiring or requesting operator assistance, the RealPresence Collaboration Server management application displays the following:



- The participant's connection *Status* changes, reflecting the help request. For details, see Table 13-9.
- The conference status changes and it is displayed with the exclamation point icon and the status "Awaiting Operator".
- The appropriate voice message is played to the relevant participants indicating that assistance will be provided shortly.

The following icons and statuses are displayed in the *Participant Status* column:

Table 13-9 *Participants List Status Column Icons and Indications*

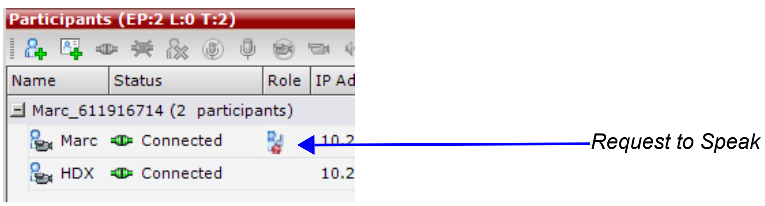
Icon	Status indication	Description
	*Awaiting Individual Assistance*	The participant has requested the operator's assistance for himself/herself.
	*Awaiting Conference Assistance*	The participant has requested the operator's assistance for the conference. Usually this means that the operator is requested to join the conference.

When the Operator moves the participant to the *Operator conference* for individual assistance the participant Status indications are cleared.

Request to Speak

Participants that were muted by the conference organizer/system operator can indicate that they want to be unmuted by entering the appropriate DTMF code.

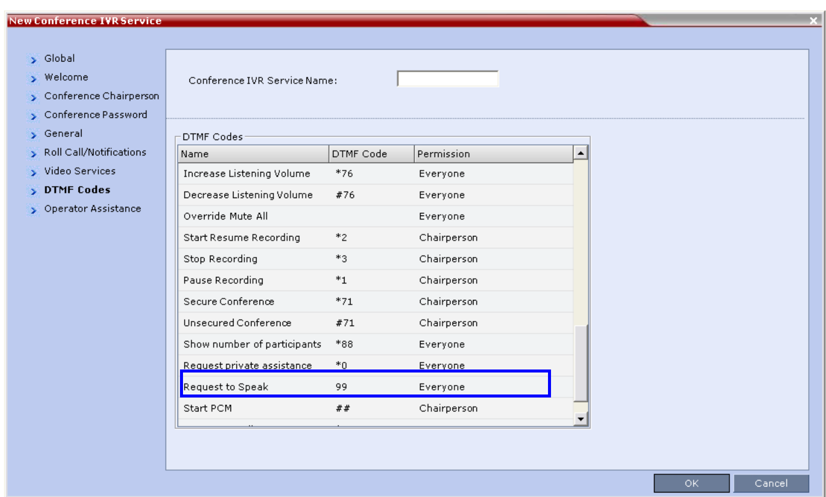
An icon is displayed in the *Role* column of the *Participants* list for 30 seconds.



Request to Speak is:

- Activated when the participant enters the appropriate DTMF code (default: **99)**.

  The DTMF code can be modified in the conference *IVR Service Properties - DTMF Codes* dialog box.

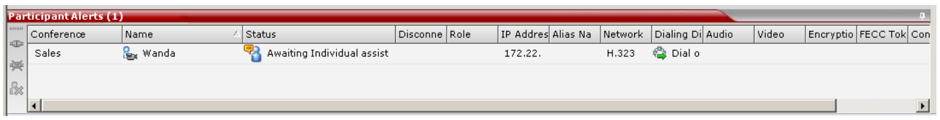


- Available for dial-in and dial-out participants.
- A participant can request to speak more than once during the conference.
- Supported in *all* conference types.
- Supported in H.323 and SIP environments.

- The duration of the icon display cannot be modified.

Participant Alerts List

The *Participant Alerts* list contains all the participants who are currently waiting for operator assistance.



Participants are automatically added to the *Participants Alerts* list in the following circumstances:

- The participant fails to connect to the conference by entering the wrong conference ID or conference password and waits for the operator’s assistance.
- The participant requests Operator’s Assistance during the ongoing conference.

This list is used as reference only. Participants can be assisted and moved to the *Operator conference* or the destination conference only from the *Participants* list of the Entry Queues or ongoing conference where they are awaiting assistance.

The participants are automatically removed from the *Participant Alerts* list when moved to any conference (including the *Operator conference*).

Participant Level Monitoring

In addition to conference information, you can view detailed information regarding the status and parameters of each listed participant, using the *Participant Properties* dialog box. Participant properties can be displayed for all participants currently connected to a conference and for defined participants that have been disconnected.

> Properties differ for IP and ISDN/PSTN participants.
> SIP SVC-based participant properties are similar to SIP AVC-based participant properties.

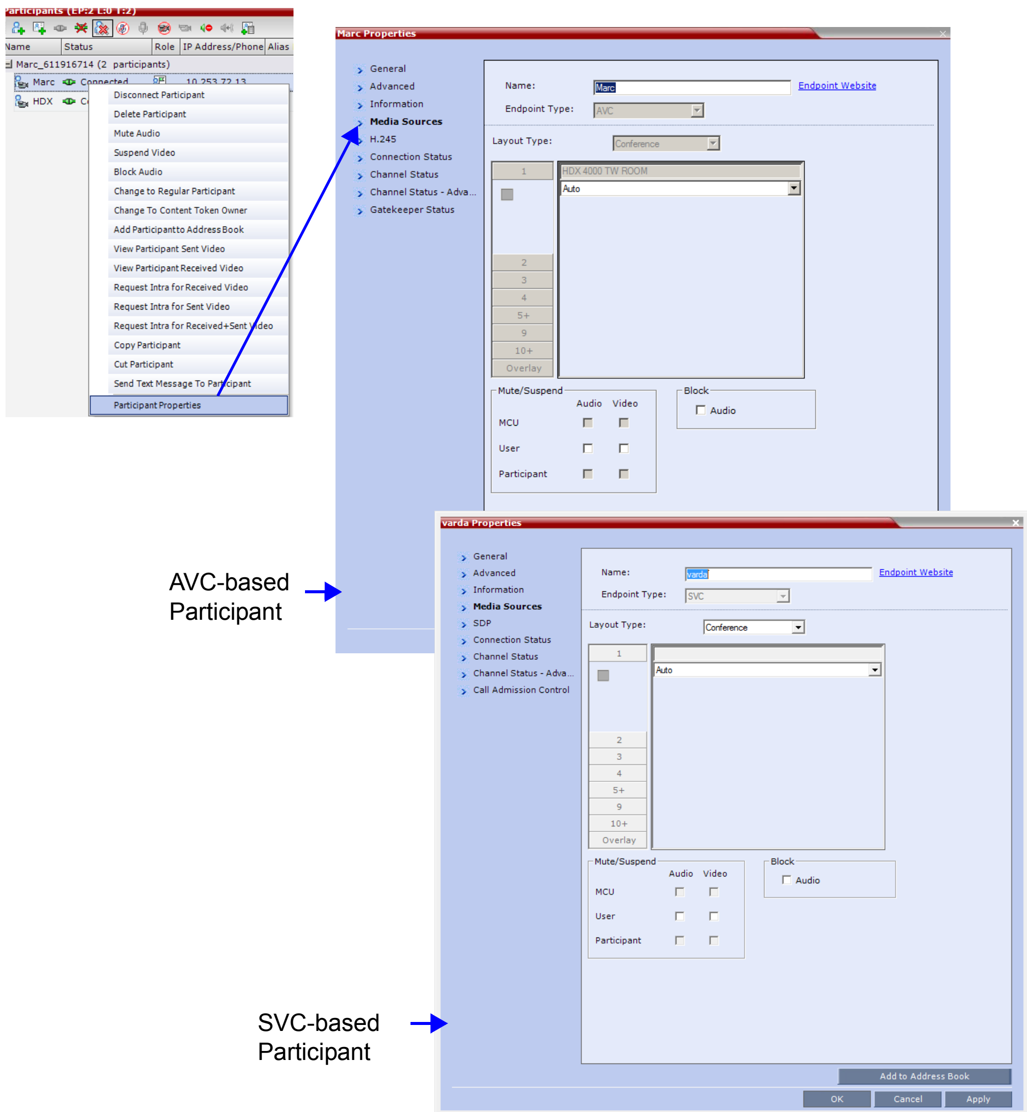
Displaying Participants Properties

To display the participant Properties:

1 In the *Participant List* pane double-click the participant entry. Alternatively, right-click a participant and then click **Participant Properties**.

The *Participant Properties - Media Sources* dialog box opens.

Viewing Permissions			
Tab	Chairperson	Operator	Administrator
Media Sources	✔	✔	✔



The *Media Sources* dialog box enables you to mute participant's audio, suspend participant's video transmission and select a personal Video Layout for the participant.

For ISDN/PSTN participants, only the following tabs are displayed in the *Participant Properties* dialog box:

- General, Advanced, Information
- Media Sources
- Connection Status
- Channel Status

The *General*, *Advanced* and *Information* tabs include the same properties for new and defined participants. For more information, see "*Adding a new participant to the Address Book Directly"* on page **8-8**.

IP Participant Properties

Table 13-10 *Participant Properties - Media Sources Parameters*

Field	Description
Name	Indicates the participant's name. **Note:** This field is displayed in all tabs.
Endpoint Website (link)	Click the Endpoint Website hyperlink to connect to the internal website of the participant's endpoint. It enables you to perform administrative, configuration and troubleshooting activities on the endpoint. The connection is available only if the IP address of the endpoint's internal site is filled in the *Website IP Address* field in the *Participant Properties - General* dialog box. **Note:** This field is displayed in all tabs (excluding ISDN/PSTN participants).
Endpoint Type	Indicates whether the participant is using an AVC-based or SVC-based endpoint. Fields, tabs and options are enabled or disabled according to the endpoint type. **Note:** This field is displayed in all tabs.
Layout Type	Indicates whether the video layout currently viewed by the participant is the Conference or Personal Layout. If *Personal Layout* is selected, you can select a Video Layout that will be viewed only by this participant.
Video Layout	Indicates the video layout currently viewed by the participant. When *Personal Layout* is selected in the *Layout Type* you can force participants to the video windows in a layout that is specific to the participant. For more information, *see RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide,* "*Changing the Video Layout of a Conference (AVC-Based Conferences)"* on page **3-56**.

Table 13-10 *Participant Properties - Media Sources Parameters (Continued)*

Field	Description
Mute/Suspend	Indicates if the endpoint's audio and/or video channels have been muted/ suspended. The entity that initiated audio mute or video suspend is also indicated. • **MCU** – Audio or Video channel has been muted/suspended by the MCU. • **User** – Channels have been muted/suspended by the RMX user. • **Participant** – Channels have been muted/suspended by the participant from the endpoint. You can also cancel or perform mute and suspend operation using these check boxes. **Note:** If the participant muted his/her audio channel, the system displays the mute icon only for H.323. This icon is not displayed for SIP participant due to SIP standard limitation.
Block	When checked, the audio transmission from the conference to the participant's endpoint is blocked, but the participant will still be heard by other participants.

2 Click the **Connection Status** tab to view the connection status, and if disconnected the cause of the disconnection. This dialog box is the same for AVC-based and SVC-based participants.

Viewing Permissions			
Tab	*Chairperson*	*Operator*	*Administrator*
Connection Status	✔	✔	✔

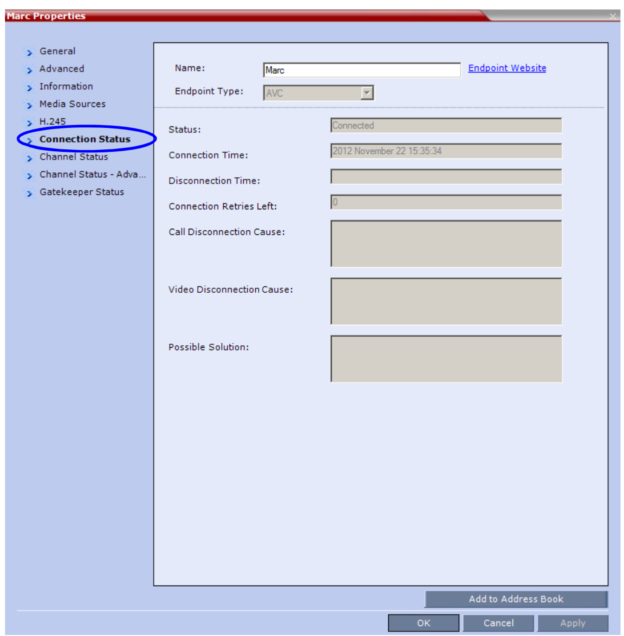


Table 13-11 *Participant Properties - Connection Status Parameters*

Field	Description
Participant Status	
Status	Indicates the connection status of the participant.

Table 13-11 *Participant Properties - Connection Status Parameters (Continued)*

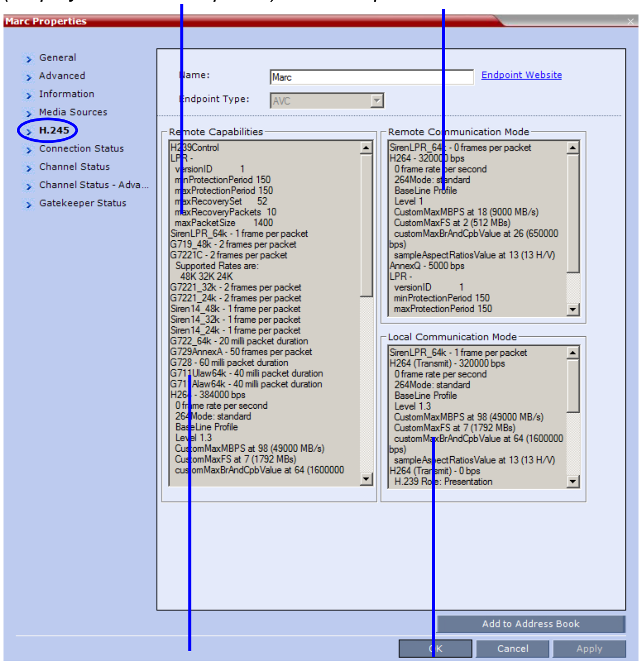
Field	Description
Connection Time	The date and time the participant connected to the conference. **Note:** The time format is derived from the MCU’s operating system time format.
Disconnection Time	The date and time the defined participant disconnected from the conference.
Connection Retries Left	Indicates the number of retries left for the system to connect defined participant to the conference.
Call Disconnection Cause	Displays the cause for the defined participant’s disconnection from the conference. See *Appendix A:* "*Disconnection Causes”* on page **A-1**.
Video Disconnection Cause	Displays the cause the video channel could not be connected. For more information, see *Appendix A:* "*Disconnection Causes”* on page **A-1**.
Possible Solution	In some cases, a possible solution is indicated to the cause of the video disconnection.

3 Click the **H.245** (H.323) or **SDP** (SIP) tab during or after the participant’s connection process to view information that can help in resolving connection issues.

LPR activity (Displayed in all three panes)

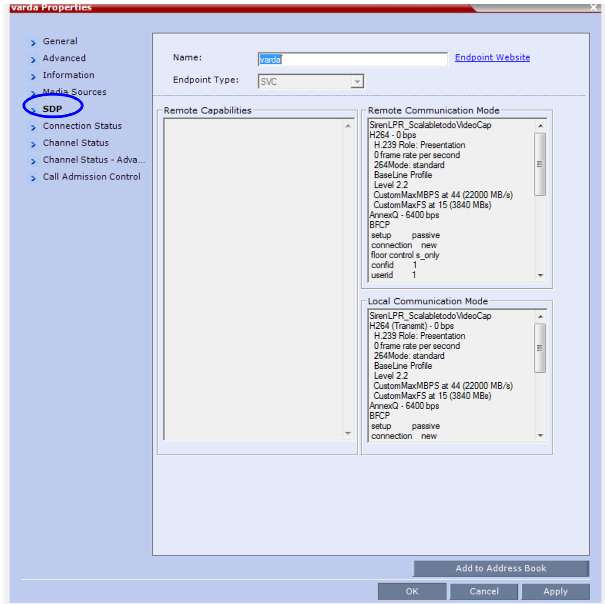
Displays the endpoint’s actual capabilities used for the connection

H.323 Participant (AVC-based|)



List’s the endpoint’s capabilities as retrieved from the remote site

Displays the MCU’s capabilities used for connection with the participant



SIP Participant (AVC-based and SVC-based)

Viewing Permissions			
Tab	*Chairperson*	*Operator*	*Administrator*
Channel Status		✔	✔

***Table 13-12** Participant Properties - H.245/SDP Parameters*

Field	Description
Remote Capabilities	Lists the participant's capabilities as declared by the endpoint.
Remote Communication Mode	Displays the actual capabilities used by the endpoint when establishing the connection with the MCU (Endpoint to MCU).
Local Communication Mode	Displays the actual capabilities used by the MCU when establishing the connection with the participant's endpoint (MCU to Endpoint).

4 Click on the **Channel Status** tab to view the status of the various channels.

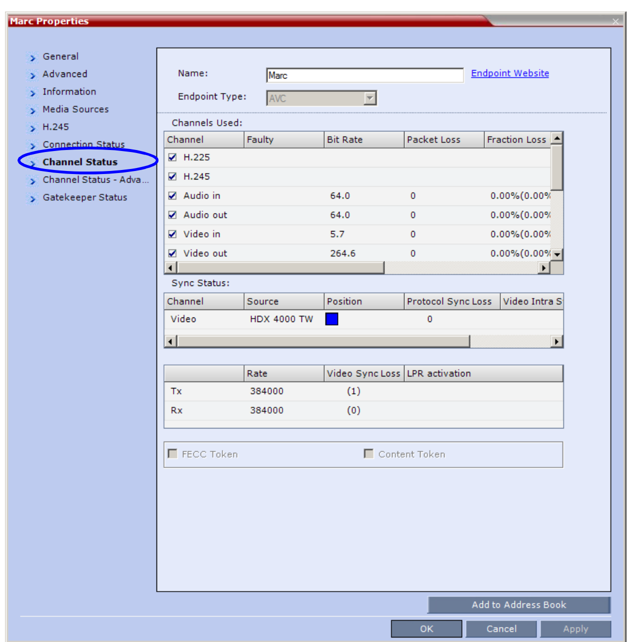


Table 13-13 *Participant Properties - Channel Status Parameters*

Field	Description
Channels Used	When checked, indicates the channel type used by the participant to connect to the conference: Incoming channels are endpoint to MCU, Outgoing channels are from MCU to endpoint. **Channels:** • *H.225/Signaling* - The call-signaling channel. • *H.245/SDP* - The Control channel. • *Audio in - Incoming audio channel* • *Audio out - Outgoing audio channel* • *Video in - Incoming video channel* • *Video out - Outgoing video channel* • *Content in* - H.239/People+Content conferences • *Content out* - H.239/People+Content conferences • *FECC in* - The incoming FECC channel is open. • *FECC out* - The outgoing FECC channel is open. **Columns:** • **Faulty** – A red exclamation point indicates a faulty channel condition. This is a real-time indication; when resolved the indication disappears. An exclamation point indicates that further investigation may be required using additional parameters displayed in the *Advanced Channel Status* tab. • **Bit Rate** – The actual transfer rate for the channel. When channel is inactive, bit rate value is 0. For example, if the participant is connected without video, the bit rate for the video channel is 0. **Note:** The CTS Audio Auxiliary channel is used only for Content. In all other cases, the bit rate shown in this column for this channel is 0. • **Packet Loss** – The accumulated count of all packets that are missing according to the RTCP report since the channel was opened. This field is relevant only during the connection stage and does not display faulty indications. • **Fraction Loss (Peak)** – The ratio between the number of lost packets and the total number of transmitted packets since the last RTCP report. *Peak* (in parentheses) indicates the highest ratio recorded since the channel was opened. • **Number of Packets** – The number of received or transmitted packets since the channel has opened. This field does not cause the display of the faulty indicator. • **Jitter (Peak)** – Displays the network jitter (the deviation in time between the packets) as reported in the last RTCP report (in milliseconds). *Peak* (in parentheses) reflects the maximum network jitter since the channel was opened. • **Latency** – Indicates the time it takes a packet to travel from one end to another in milliseconds (derived from the RTCP report).

Table 13-13 Participant Properties - Channel Status Parameters (Continued)

Field	Description
Sync Status	***Channel*** - The channel type: Video or Content. ***Source*** - The name of the participant currently viewed by this participant. ***Position*** - The video layout position indicating the place of each participant as they appear in a conference. ***Protocol Sync Loss*** - Indicates whether the system was able to synchronize the bits order according to the selected video protocol. ***Video Intra Sync*** - Indicates whether the synchronization on a video Intra frame was successful. ***Video Resolution*** - The video resolution of the participant.
Rx - Rate	The received line rate.
Tx - Rate	The transmitted line rate.
Tx - Video Sync Loss	When checked, indicates a video synchronization problem in the outgoing channel from the MCU. The counter indicates the sync-loss count.
Rx - Video Sync Loss	When checked, indicates a video synchronization problem in the incoming channel from the endpoint. The counter indicates the sync-loss count.
Tx - LPR Activation	When checked, indicates LPR activation in the outgoing channel.
Rx - LPR Activation	When checked, indicates LPR activation in the incoming channel.
FECC Token	When checked, indicates that the participant is the holder of the FECC Token.
Content Token	When checked, indicates that the participant is the holder of the Content Token.

Viewing Permissions			
Tab	*Chairperson*	*Operator*	*Administrator*
Channel Status Advanced			✔

5 Click the **Channel Status Advanced** tab to view additional information for selected audio and video channels.

In the *Channel Status - Advanced* tab, channels can be selected for viewing additional information:

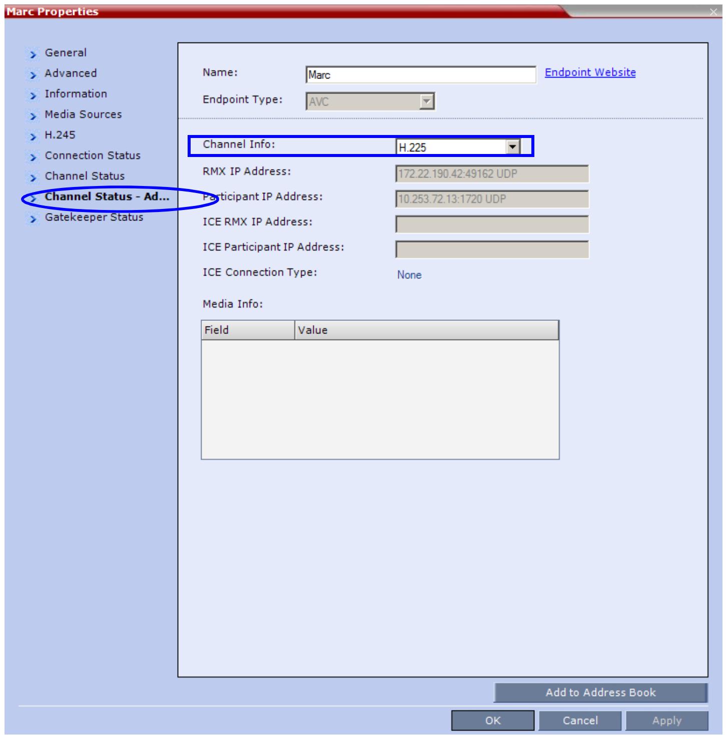


Table 13-14 Participant Properties - Channel Status Advanced Parameters

Field	Description
Channel Info	Select a channel to view its information: • H.225 • H.245 • Audio in • Audio out • Video in • Video out • Content in • Content Out • SIP BFCP TCP IN
RMX IP Address	The IP address and the transport protocol (TCP/UDP) of the MCU to which the participant is connected and the port number allocated to the participant incoming media stream on the MCU side.

Table 13-14 *Participant Properties - Channel Status Advanced Parameters (Continued)*

Field	Description
Participant IP Address	The IP address and the transport protocol (TCP/UDP) of the participant and the port number allocated to the media stream on the participant side.
ICE RMX IP Address	The IP address, port number, and transport protocol of the MCU used to pass through the media when ICE is functional. See Appendix H, "*Participant Properties - ICE Connection Parameters"*on page **H-66**.
ICE Participant IP Address	The IP address, port number, and transport protocol of the endpoint used to pass through the media when ICE is functional. See Appendix H, "*Participant Properties - ICE Connection Parameters"*on page **H-66**.
ICE Connection Type	Indicates the type of connection between the RMX and the participant in the ICE environment:• • **Local** (or Host) - The endpoint (Remote) is on the same network as the RMX and the media connection is direct, using local addresses. • **Relay** - Media between the RMX and the participant passes through a media relay server. • **Firewall** - Media connection between the RMX and the participant is done using their external IP addresses (the IP addresses as seen outside of the local network).
Media Info	This table provides information about the audio and video parameters, such as video algorithm, resolution, etc. For more information, see *Appendix E:* "*Participant Properties Advanced Channel Information"* on page **E-1**.
RTP Statistics	This information may indicate problems with the network which can affect the audio and video quality. For more information, see *Appendix E:* "*Participant Properties Advanced Channel Information"* on page **E-1**.

6 **Optional for H.323 AVC-based participants.** Click the **Gatekeeper Status** tab to view its parameters.

Viewing Permissions			
Tab	*Chairperson*	*Operator*	*Administrator*
Gatekeeper Status	✔	✔	✔

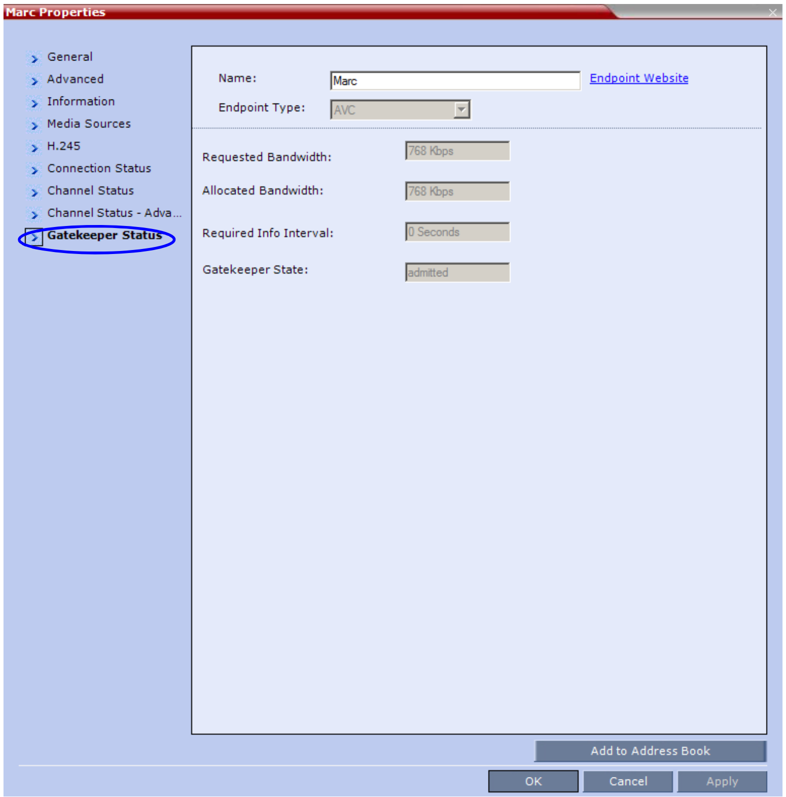


***Table 13-15** Participant Properties - Gatekeeper Status Parameters*

Field	Description
Requested Bandwidth	The bandwidth requested by the MCU from the gatekeeper.
Allocated Bandwidth	The actual bandwidth allocated by the gatekeeper to the MCU.
Required Info Interval	Indicates the interval, in seconds, between registration messages that the MCU sends to the gatekeeper to indicate that it is still connected.
Gatekeeper State	Indicates the status of the participant's registration with the gatekeeper and the bandwidth allocated to the participant. The following statuses may be displayed: • ***ARQ*** – Admission Request - indicates that the participant has requested the gatekeeper to allocate the required bandwidth on the LAN. • ***Admitted*** – indicates that the gatekeeper has allocated the required bandwidth to the participant. • ***DRQ*** – Disengage Request – the endpoint informs the gatekeeper that the connection to the conference is terminated and requests to disconnect the call and free the resources. • ***None*** – indicates that there is no connection to the gatekeeper.

7 **Optional for SIP AVC-based and SVC-based participants.** Click the **Call Admission Control** tab to view its parameters.

Viewing Permissions			
Tab	Chairperson	Operator	Administrator
Gatekeeper Status	✔	✔	✔

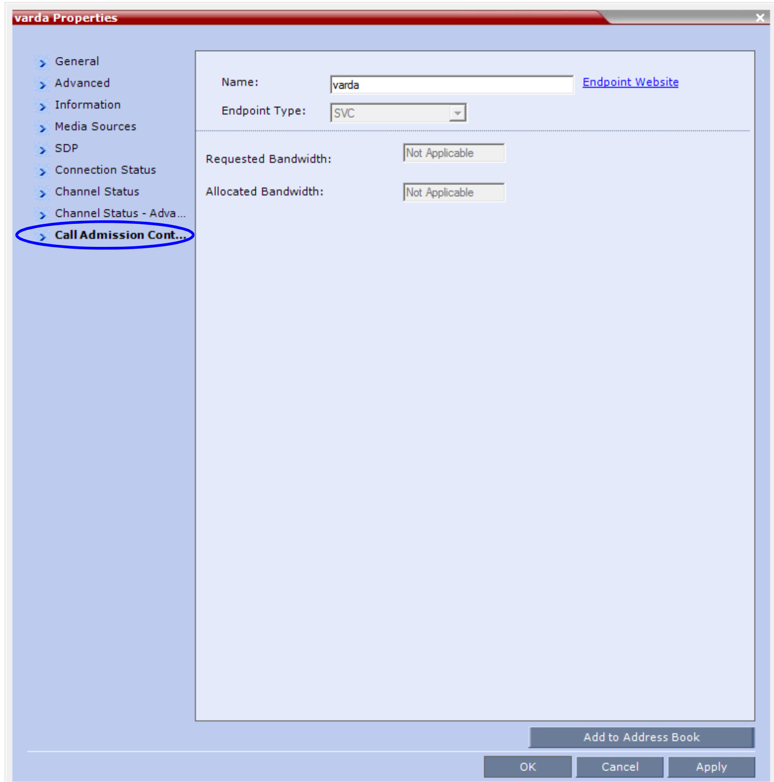


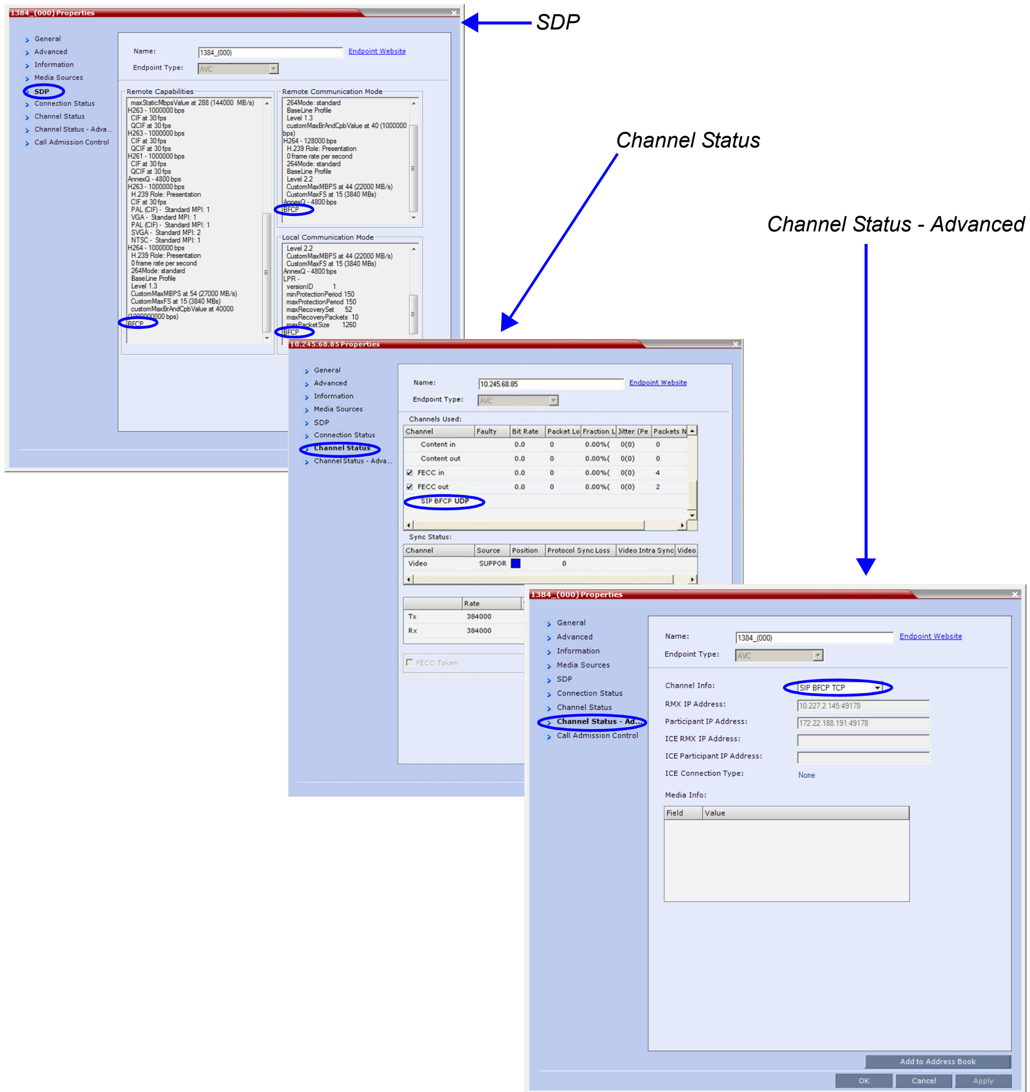
Table 13-16 Participant Properties - Gatekeeper Status Parameters

Field	Description
Requested Bandwidth	The bandwidth requested by the MCU from the SIP server.
Allocated Bandwidth	The actual bandwidth allocated by the SIP server to the MCU.

Monitoring SIP BFCP Content

In the SIP *Participant Properties* dialog box, *BFCP* status information appears in:

- All three panes of the *SDP* tab.
- The *Channel Status* tab.
- The *Channel Status -Advanced* tab.



For more information see "*Participant Level Monitoring*" on page **13-21**.

Monitoring ISDN/PSTN Participants

Using the *Participant Properties* dialog box, you can monitor and verify the properties of an ISDN/PSTN participant. The dialog box's tabs contain information that is relevant to the participant's status only while the conference is running and is used to monitor the participant's status when connection problems occur.

Maximum line rate at which ISDN endpoints can connect to a conference is 768 kbps.

Table 13-17 lists the audio algorithms that are supported for ISDN participants according to their connection bit rate:

Table 13-17 *Supported Audio Algorithms vs Bit Rate*

	Bit Rate		
	96Kbps (and Lower)	**128Kbps – 192Kbps**	**256Kbps (and Higher)**
Audio Algorithm	G722.1 16K	G722.1 C 32K	G722.1 C 48K
	G722.1 C 24K	G722.1 C 24K	G722.1 C 32K
	Siren14 24K	Siren14 32K	G722.1 C 24K
	G722 48K	Siren14 24K	Siren14 48K
	G722 56K	G722.1 32K	Siren14 32K
	G722 64K	G722.1 24K	Siren14 24K
	G711 56K	G722 48K	G722.1 32K
	G711 64K	G722 56K	G722.1 24K
		G722 64K	G722.1 16K
		G711 56K	G722 48K
		G711 64K	G722 56K
			G722 64K
			G711 56K
			G711 64K

To view the participant properties during a conference:

1 In the *Participants* list, right click the desired participant and select **Participant Properties**.

The *Participant Properties - Media Sources* dialog box is displayed.

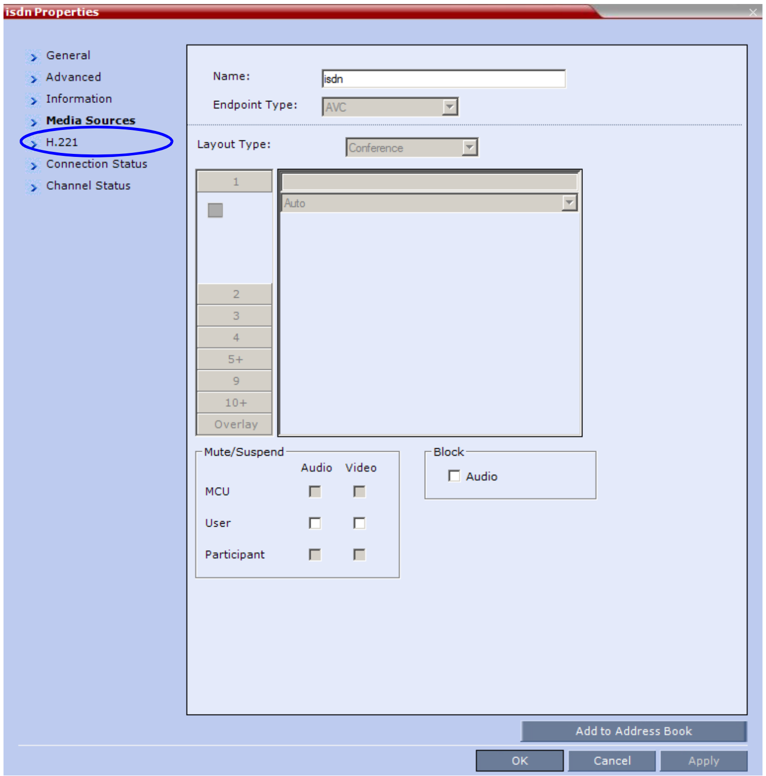


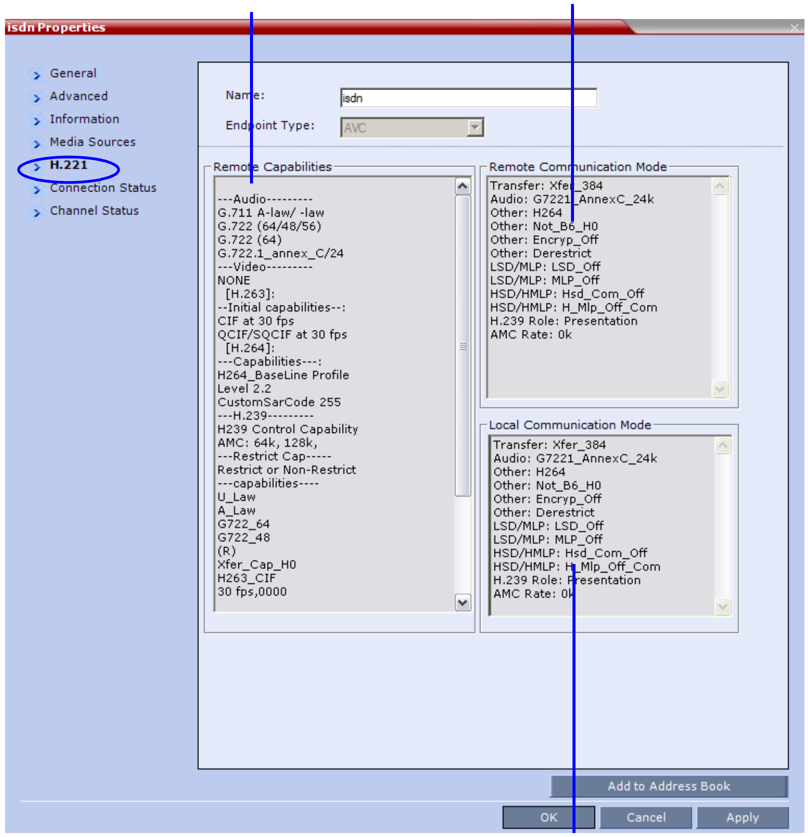
Table 13-18 *ISDN/PSTN Participant Properties - Media Sources*

Field	Description
Mute/Suspend	Indicates if the endpoint’s audio and/or video channels from the endpoint have been muted/suspended. The entity that initiated audio mute or video suspend is also indicated. • **MCU** – Audio or Video channel has been muted/suspended by the MCU. • **User** – Channels have been muted/suspended by the RMX user. • **Participant** – Channels have been muted/suspended by the participant from the endpoint. You can also cancel or perform mute and suspend operation using these check boxes.
Block (Audio)	When checked, the audio transmission from the conference to the participant’s endpoint is blocked, but the participant will still be heard by other participants.

2 Click the **H.221** tab to view additional information that can help to resolve connection issues.

List's the endpoint's capabilities as retrieved from the remote site

Displays the endpoint's actual capabilities used for the connection



Displays the MCU's capabilities used for connection with the participant

Table 13-19 *Participant Properties - H.221 Parameters*

Field	Description
Remote Capabilities	Lists the participant's capabilities as declared by the endpoint.
Remote Communication Mode	Displays the actual capabilities used by the endpoint when establishing the connection with the MCU (Endpoint to MCU).
Local Communication Mode	Displays the actual capabilities used by the MCU when establishing the connection with the participant's endpoint (MCU to Endpoint).

3 Click the **Connection Status** tab to view general information regarding the participant connection and disconnection causes of the participant to the conference.

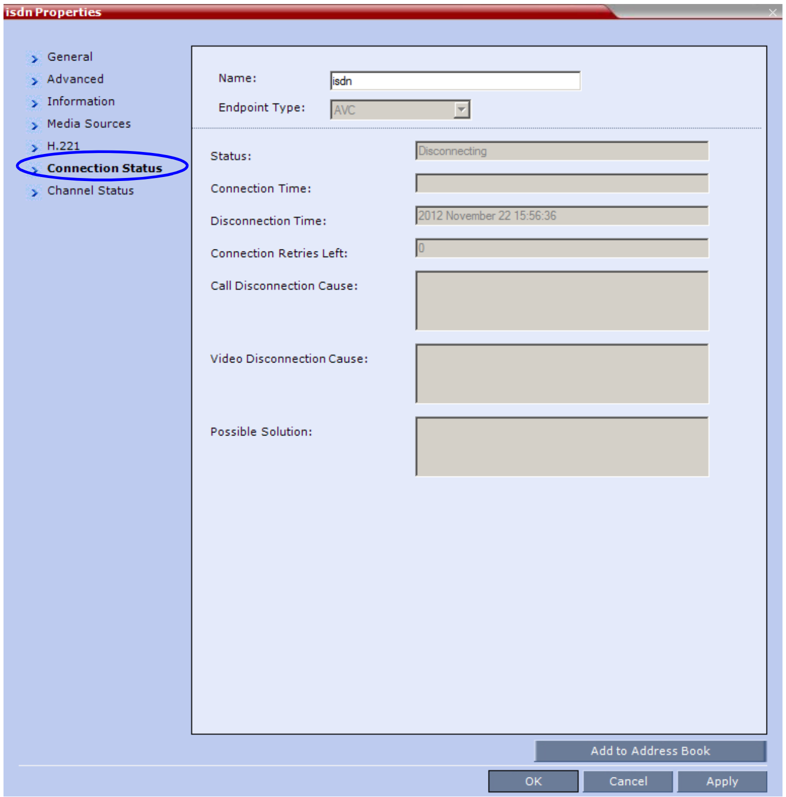


Table 13-20 *ISDN/PSTN Participant Properties - Connection Status*

Field	Description
Status	Indicates the connection status of the participant to the conference. If there is a problem, the appropriate status is displayed, for example, Disconnected.
Connection Time	The date and time the participant connected to the conference.
Disconnection Time	The date and time the participant was disconnected from the conference.
Connection Retries Left	Indicates the number of retries left for the system to connect the participant to the conference.
Call Disconnection Cause	For a full list of *Disconnection Causes*, see "*ISDN Disconnection Causes"* on page **A-7**.

4 Click the **Channel Status** tab to view the status of a participant's channels.

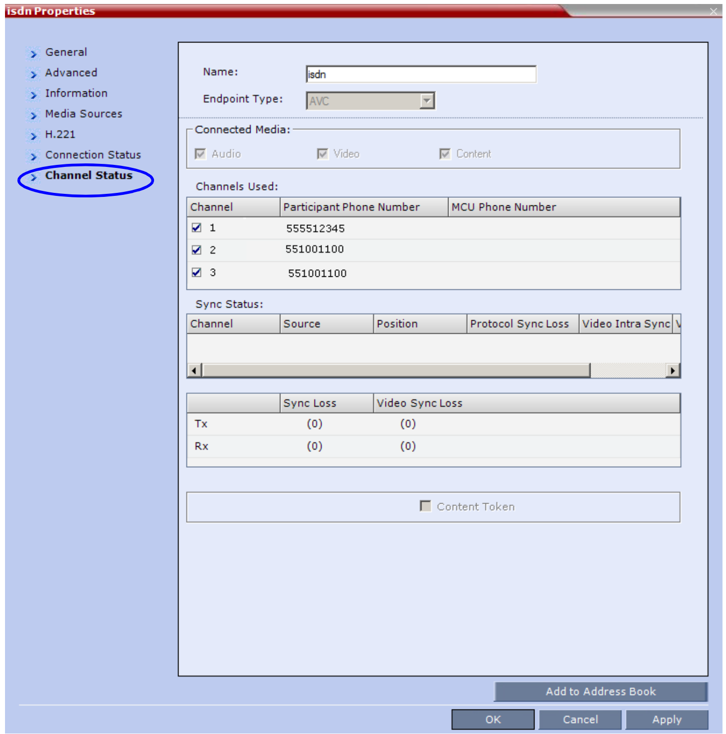


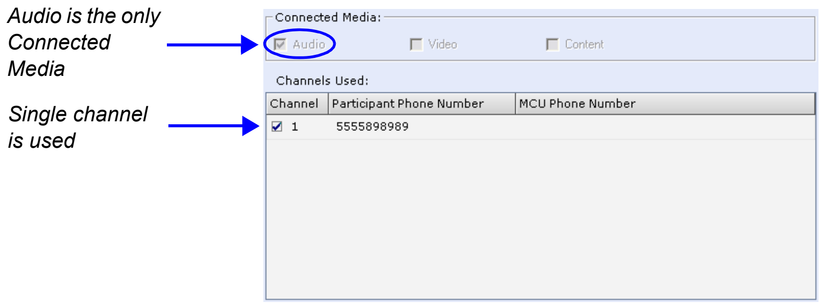
Table 13-21 *ISDN/PSTN Participant Properties - Channel Status*

Field	Description
Connected Media	Indicates if the participant is connected with Audio, Video and Content media channels.
Channels Used	• **Channel** – Indicates the channel used by the participants and whether the channel is connected (indicated with a check mark) or disconnected. • **Participant Phone Number** – In a dial-in connection, indicates the participant's CLI (Calling Line Identification) as identified by the MCU. In a dial-out connection, indicates the participant's phone number dialed by the MCU for each channel. • **MCU Phone Number** – In a dial-in connection, indicates the MCU number dialed by the participant. In a dial-out connection, indicates the MCU (CLI) number as seen by the participant. This is the number entered in the MCU Number field in the Network Service.
Tx - Video Sync Loss	When checked, indicates a video synchronization problem in the outgoing channel from the MCU. The counter indicates the sync-loss count.
Rx - Video Sync Loss	When checked, indicates a video synchronization problem in the incoming channel from the endpoint. The counter indicates the sync-loss count.

Table 13-21 *ISDN/PSTN Participant Properties - Channel Status*

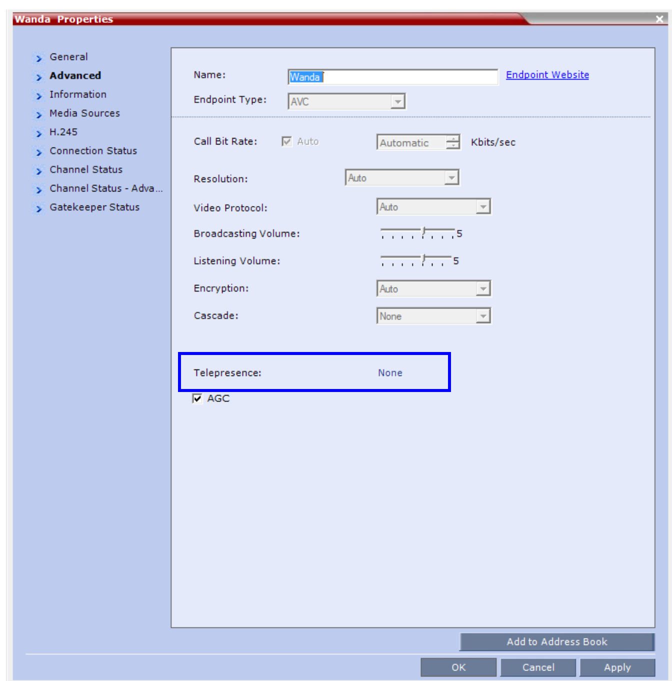
Field	Description
Content Token	A check mark indicates that the participant is the current holder of the Content Token.

The *Connected Media* and *Channels Used* fields of an *Audio Only* participant are displayed as follows:



Monitoring Telepresence Participant Properties

A *Telepresence* status indicator is displayed in the *Participant Properties - Advanced* tab when monitoring conference participants.



The *Telepresence* mode of the participant is indicated:

- *RPX* - the participant's endpoint is transmitting 4:3 video format.
- *TPX* - the participant's endpoint is transmitting 16:9 video format.
- *None* - the participant's endpoint is neither *RPX* nor *TPX*.

14

Recording Conferences

> Conference recording is available in AVC Conferencing Mode only.

Conferences running on the *RMX* can be recorded using a *Polycom® RSS™ Recording and Streaming Server* (*RSS*).

The recording system can be installed at the same site as the conferencing *MCU* or at a remote site. Several *MCU's* can share the same recording system.

Recording conferences is enabled via a *Recording Link*, which is a dial-out connection from the conference to the recording system.

Recording can start automatically, when the first participant connects to a conference, or on request, when the RMX user or conference chairperson initiates it.

Multiple Recording Links may be defined.

Conference Recording Links can be associated on the RMX with *Virtual Recording Rooms* (*VRR*), created and saved on the *Polycom® RSS™ 4000 Version 6.0 Recording and Streaming Server* (*RSS*).

Each *Recording Link* defined on the RMX can be given a descriptive name and can be associated with one *VRR* saved on the *Polycom RSS 4000*.

The following guidelines apply:

- A *Recording Link* that is being used by an ongoing conference cannot be deleted.
- A *Recording Link* that is assigned to a *Profile* cannot be deleted.
- The *Recording Link* does not support H.264 High Profile.
- While a *Profile* s being used in an ongoing conference, it cannot have a different *Recording Link* assigned to it.
- Up to 100 Recording Links can be listed for selection in the Conference Profile.
- *Multiple Recording Links* are supported in *Continuous Presence* and *Video Switched* conferences.
- The number of *Recording Links* available for selection is determined by the value of the **MAXIMUM_RECORDING_LINKS** *System Flag* in *system.cfg*. Default value is 20 Recording Links.
- The recording link can be encrypted when recording from an encrypted conference to the RSS that is set to encryption. For more details, see "*Recording Link Encryption"* on page **14-7**.

Creating Multiple Virtual Recording Rooms on the RSS

If the environment includes a *Polycom® RSS™ 4000 Version 6.0 Recording and Streaming Server (RSS)* and you want to associate *Recording Links* on the RMX with *Virtual Recording Rooms* (*VRR*), created and saved on the *Polycom® RSS™ 4000 Version 6.0* perform the following operations on the *RSS*:

1 Modify the parameters of a recording *Template* to meet the recording requirements.

2 Assign the modified recording *Template* to a *VRR*. The recording and streaming server will assign a number to the *VRR*.

3 Repeat Step 1 and Step 2 for each *VRR* to create additional *VRR*s.

For more information see the *RSS 4000 Version 6.0 User Guide.*

Configuring the RMX to Enable Recording

To make recording possible the following components you must be configured on the RMX:

- *Recording Link* – defines the connection between the conference and the recording system.
- *Recording-enabled Conference IVR Service* – recording *DTMF* codes and messages must be set in the *Conference IVR* Service to enable "recording-related" voice messages to be played and to allow the conference chairperson to control the recording process using *DTMF* codes.
- *Recording-enabled Profile* – recording must be enabled in the *Conference Profile* assigned to the recorded conference.

If *Multiple Recording Links* are being defined for *Virtual Recording Rooms* (*VRRs*), created and saved on the *Polycom® RSS™ 4000 Version 6.0*, the **MAXIMUM_RECORDING_LINKS** *System Flag* in *system.cfg* can be modified to determine the number of *Recording Links* available for selection.

- **Range:** 20 - 100
- **Default:** 20

The flag value can be modified by selecting the *System Configuration* option from the *Setup* menu. For more information, see "*Modifying System Flags"* on page **22-1**.

Defining the Recording Link

The *Recording Link* is defined once and can be updated when the *H.323* alias or the IP address (of the recording system) is changed. Only one *Recording Link* can be defined in the RMX. Its type must be *H.323*.

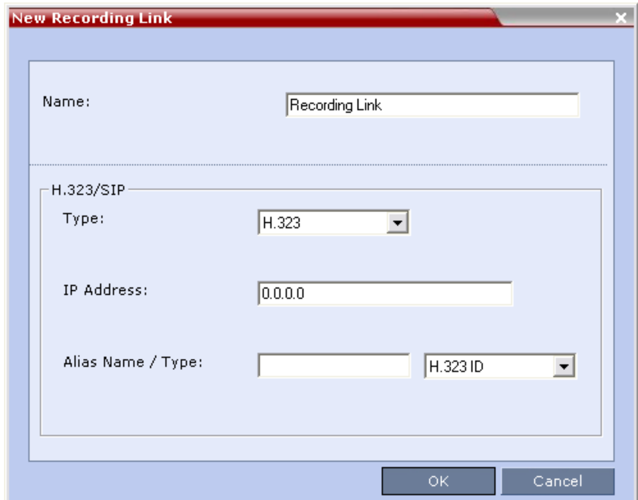
In *Multiple Networks* Configuration, Recording Links use the default Network Service to connect to conferences, therefore the recording system must be defined on the default IP Network Service to enable the recording.

To define a Recording Link:

1 In the *RMX Management* pane, click **Recording Links** ( ).

2 In the *Recording Links* list, click the **New Recording Link** ( ) button.

The *New Recording Link* dialog box is displayed.



3 Define the following parameters:

Table 14-1 *Recording Link Parameters*

Parameter	**Description**
Name	Displays the default name that is assigned to the Recording Link. If multiple Recording Links are defined, it is recommended to use a descriptive name to be indicate the VRR to which it will be associated. Default: *Recording Link*
Type	Select the network environment: • H.323 • SIP
IP Address	• If no gatekeeper is configured, enter the IP Address of the RSS. Example: If the RSS IP address is 173.26.120.2 enter `173.26.120.2.` • If a gatekeeper is configured, you can either enter the IP address or an alias (see the alias description).
Alias Name	If using the endpoint's alias instead of IP address, first select the alias type and then enter the endpoint's alias. If you are associating this recording link to a VRR on the RSS, define the alias as follows: • If you are using the RSS IP address, enter the VRR number in the Alias field. For example, if the VRR number is 5555, enter **5555**. • Alternatively, if the *Alias Type* is set to **H.323 ID**, enter the RSS IP address and the VRR number in the format: **<RSS_IP_Address>##<VRR number>** For example: If the RSS IP is 173.26.120.2 and the VRR number is 5555, enter **173.26.120.2##5555**
Alias Type	Depending on the format used to enter the information in the IP address and Alias fields, select **H.323 ID** or **E.164** (for multiple Recording links). **E-mail ID** and **Participant Number** are also available.

4 Click **OK**.

The Recording Link is added to the RMX unit.

Enabling the Recording Features in a Conference IVR Service

To record a conference, a *Conference IVR Service* in which the recording messages and DTMF codes are activated must be assigned to the conference. The default *Conference IVR Service* shipped with the RMX includes the recording-related voice messages and default DTMF codes that enable the conference chairperson to control the recording process from the endpoint. You can modify these default settings.

To modify the default recording settings for an existing Conference IVR Service:

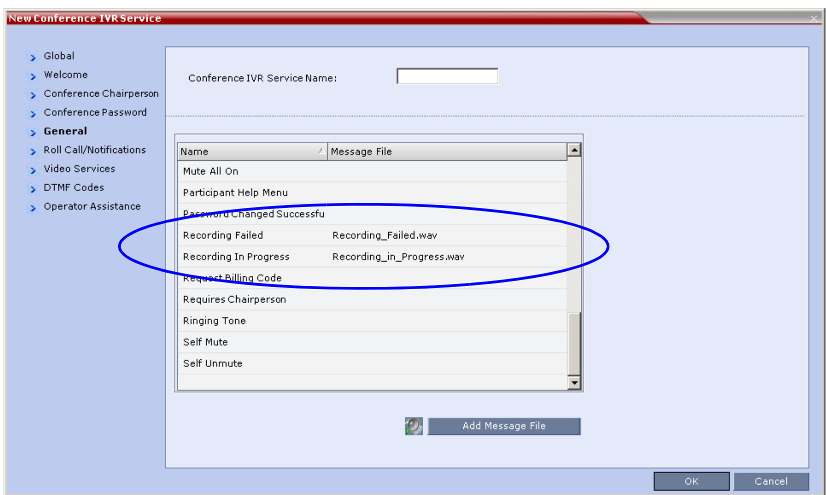
1 In the *RMX Management* pane, click the **IVR Services** ( ) button.

The IVR Services are listed in the *IVR Services* list pane.

2 To modify the default recording settings, double-click the Conference IVR Service or right-click and select **Properties**.

The *Conference IVR Service Properties* dialog box is displayed.

3 To assign voice messages other than the default, click the **General** tab and scroll down the list of messages to the recording messages.



4 Select the *Recording In Progress* message, and then select the appropriate message file (by default, Recording_in_Progress.wav) from the file list to the right of the field.

5 Select the *Recording Failed* message, and then select the appropriate message file (by default, Recording_Failed.wav) from the file list to the right of the field.

6 To modify the default DTMF codes, click the **DTMF Codes** tab.

7 To modify the DTMF code or permission for a recording function:

a Select the desired DTMF name (Start, Stop or Pause Recording), click the DTMF code entry and type a new code.

Table 14-2 Default DTMF Codes assigned to the recording process

Recording Operation	DTMF Code	Permission
Start or Resume Recording	***3**	Chairperson
Stop Recording	***2**	Chairperson
Pause Recording	***1**	Chairperson

b In the *Permission* entry, select whether this function can be used by all conference participants or only the chairperson.

8 Click **OK**.

Enabling the Recording in the Conference Profile

To be able to record a conference, the recording options must be enabled in the *Conference Profile* assigned to it. You can add recording to existing *Profiles* by modifying them.

To enable recording for a conference:

1 In the *RMX Management* pane, click the **Conference Profiles** ( ) button.

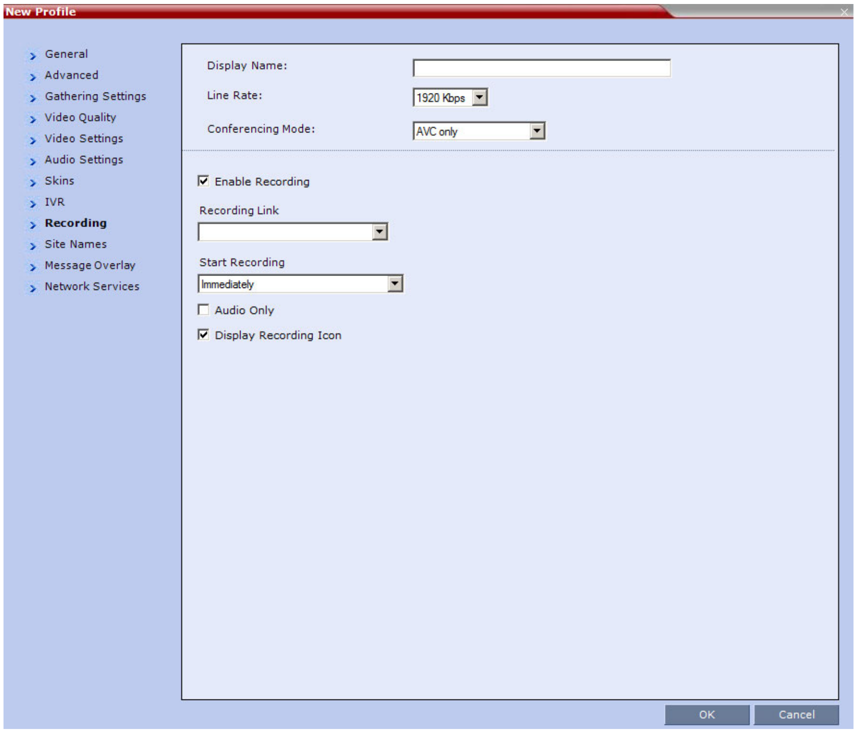
The *Conference Profiles* list is displayed.

2 Create a new profile by clicking the **New Profile** ( ) button or modify an existing profile by double-clicking or right-clicking an existing profile and then selecting **Profile Properties**.

If creating a new profile, complete the conference definition. For more information on creating Profiles see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *Defining New Profiles* on page 2-18.

3 In the *Profile Properties* dialog box, click the **Recording** tab.

4 Select the **Enable Recording** check box.



5 Define the following parameters:

Table 14-3 *Conference Profile Recording Parameters*

Parameter	Description
Enable Recording	Select to enable Recording Settings in the dialog box.
Recording Link	Select a recording link for the conference from the list.
Start recording	Select one of the following: • **Immediately** – conference recording is automatically started upon connection of the first participant. • **Upon Request** – the operator or chairperson must initiate the recording (manual).
Audio only	Select this option to record only the audio channel of the conference. **Note:** An *Audio Only* Recording Link cannot be used to record a conference if there are no Voice resources allocated in the *Video/Voice Port Configuration*.
Display Recording Icon	Select this option to display *Recording Indication* to all conference participants informing them that the conference is being recorded. The recording icon is replaced by a *Paused* icon when conference recording is paused.

6 Click **OK**.
Recording is enabled in the *Conference Profile*.

Recording Link Encryption

The Recording Link can be encrypted when recording an encrypted conference. The encryption of the *Recording Link* is enabled when *Encryption* is selected in the *Conference Profile* on the RMX and on the RSS, and the system flag **ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF** is set to **NO**.

Recording Link Encryption Guidelines:

- The *Recording Link* connection type must be H.323.
- The *Recording Link* uses the *AES* encryption format.
- The *RSS 2000/4000* recorder must be set to support encryption. The following *RSS* recorders support encryption:
  - *RSS 4000* version 5.0 with “upgrade package_1647_Release version” installed
  - *RSS 2000* with version 4.0.0.001 360 installed

  For more information see the *RSS 2000/4000 User Manual*.
- Encryption must be selected in the *Conference Profile.*

Recording Link Encryption Flag Setting

Recording Links are treated as regular participants, however if the ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF *System Flag* is set to YES a non-encrypted *Recording Link* is to be allowed to connect to an encrypted conference.

Table 14-4 summarizes the connection possibilities for a *Recording Link* that is to be connected to a conference for each of the conference *profile* and *Entry Queue* encryption options.

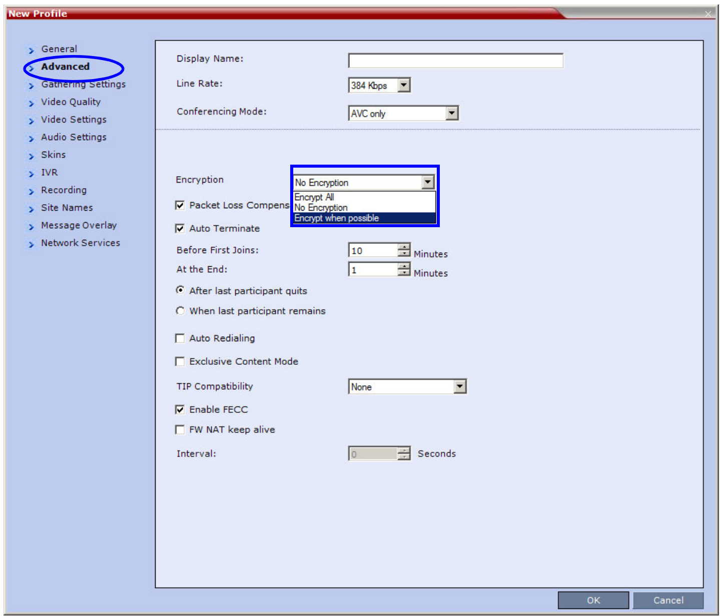
Table 14-4 Connections by Recording Link and Conference Encryption Settings

Conference Profile Setting	Recording Link Connection Status according to flag: ALLOW_NON_ENCRYPT_RECORDING_ LINK_IN_ENCRYPT_CONF	
	YES	NO
Encrypt All	Connected encrypted if possible, otherwise connected non-encrypted.	Connected only if encrypted, otherwise disconnected.
No Encryption	Connected non-encrypted.	Connected non-encrypted.
Encrypt when possible	Connected encrypted if possible, otherwise connected non-encrypted.	Connected encrypted if possible, otherwise connected non-encrypted.

Recording Link Settings

The recording of encrypted conferences via an encrypted *Recording Link* is enabled in the *Conference Profile* by:

- Selecting the *Encryption* option (**Encrypt All** or **Encrypt when Possible**) in the *Advanced* tab.



  For more details, see "*Media Encryption (AVC Only)"* on page **4-40**.

- Setting the Recording options in the *Recording* tab. For more details, see "*Enabling the Recording in the Conference Profile"* on page **14-5**.

Managing the Recording Process

When a conference is started and recording is enabled in its *Profile*, the system will automatically start the recording if the *Start Recording* parameter is set to *immediately*. If it is set to *Upon Request*, the system waits for the chairperson or RMX user's request. Once the recording is initiated for a conference, the MCU connects to the recording device (*RSS 2000*) using the default *Recording Link*. The connection that is created between the conference and the recording device is represented as a special participant (Recording) whose name is the *Recording Link*. Once the recording has started, the recording process can be stopped and restarted from the Chairperson's endpoint (using DTMF codes) or from the *RMX Web Client*. After the recording process has finished, the recording can be identified in the *RSS 2000* by its RMX conference name.

> A conference participant and the *Recording Link* cannot have identical names, otherwise the recording process will fail.

Recording Link Layout

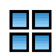
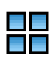
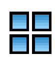
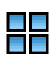
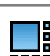
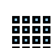
When the video layout of the conference is set to *Auto Layout*, the recording of the conference will now include all the conference participants and not n-1 participants as in previous versions.

In the new *Auto Layout* algorithm, the *Recording Link* is counted as a "participant" and therefore it is excluded from the layout display used for the recording. The layout used for the other participants will behave as in the "standard" *Auto Layout* behavior.

The *Recording Link Layout* can be changed during an ongoing conference in the same manner as for any other conference participant. For more information see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, *"Participant Level Monitoring"* on page **13-21**.

The default settings for *Auto Layout* for the conference and the *Recording Link* are summarized in the following table:

Table 15 *Recording Link Default Layout Settings (Auto Layout Mode)*

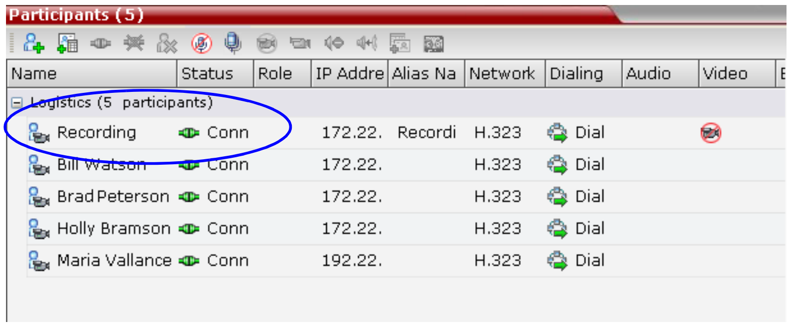
Participants	Conference Auto Layout Default Settings	Recording Link Auto Layout Settings
0	Not applicable	Not applicable
1		
2		
3		
4		
5		
6		
7		
8		
9		
10 or more		

The default settings for *Auto Layout* of the *Recording Link* cannot be changed, and the *Auto Layout* flags do not apply to the *Recording Link Auto Layout* default settings.

Using the RealPresence Collaboration Server Web Client to Manage the Recording Process

To manage the recording process using the right-click menu:

>> Right-click the *Recording* participant in the conference and select from one of the following options:



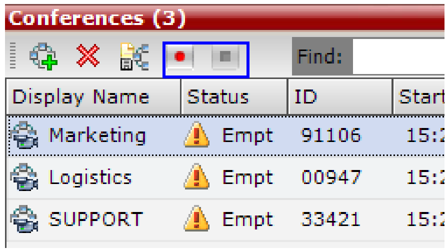
The Recording participant does not support H.264 High Profile. If recording a conference set to H,264 High Profile, the Recording participant connects as Audio Only and records the conference Audio while displaying the recording icon for the conference.

***Table 14-1** Recording Participant Right-click Options*

Name	Description
Start	Starts recording. When recording has started, this option toggles with the *Pause* option.
Pause	Pauses the recording of the conference without disconnecting. When the Recording is Paused, this option toggles with the *Start* option.
Resume	Resumes the recording of the conference. The Resume option toggles with the *Pause* option when it is used.
Stop	Stops the recording. **Note:** The Stop button is only enabled when the Recording is *Started* or *Paused*.
Suspend Video	The Suspend Video option prevents the incoming video of the recording link participant to be part of the conference layout. The Recording Link participant is set by default to Suspend Video. The Suspend Video option toggles with the Resume Video option.
Resume Video	The Resume Video option enables the incoming video of the recording link participant to be part of the conference layout. This feature may be used to play back previously recorded video or audio feeds in the conference layout. For more information, see the RSS 2000 User Guide.
Participant Properties	The Participant Properties option displays viewing only information for monitoring, e.g. communication capabilities and channels used to connect to the conference. Users will not be able to perform any functional requests from this window, i.e. disconnect, change layout and mute.

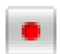
To manage the recording process using the Conference toolbar:

>> In the *Conferences* pane, click one of the following buttons in the Conference tool bar.



The recording buttons will only be displayed in the conference tool bar for a conference that is recording-enabled.

***Table 14-2** Conferences List - Recording Tool bar buttons*

Button	Description
	Start/Resume recording. This button toggles with the *Pause* button.
	Stop recording.
	Pause recording. This button toggles with the *Start/Resume* button.

Using DTMF Codes to Manage the Recording Process

By entering the appropriate DTMF code on the endpoint, the chairperson can **Stop** the recording (*74), **Pause** it (*75), or **Start/Resume** the recording (*73). For more information on managing the recording process via DTMF codes, see the *RSS 2000 User's Guide*.

Conference Recording with Codian IP VCR

Conference recording is available with *Codian VCR 2210, VCR 2220* and *VCR 2240*.

Recording between the RMX and the *Codian VCR* is enabled by adding an IP participant to the recorded conference that acts as a link between the conference and the recording device. This participant is identified as a recording link to the Codian *VCR* according to the product ID sent from the *VCR* during the connection phase, in the call setup parameters.

The video channel between the conference and the recording device is unidirectional where the video stream is sent from the conference to the recorder.

If the *Codian VCR* opens a video channel to the conference - this channel is excluded from the conference video mix.

To record a conference running on the RMX using Codian recorder:

>> In the conference, define or add a dial-out participant using the *Codian VCR* IP address as the address for dialing.

Once added to the conference, the *MCU* automatically connects the participant (the link to *Codian VCR*) and the recording is automatically started on the *Codian VCR*.

A connection can also be defined on the *Codian VCR*, dialing into the recorded conference using the *MCU* prefix and the *Conference ID* as for any other dial-in participant in the conference.

Monitoring the recording participant:

This connection is monitored as any other participant in the conference. The connection can also be monitored in the *Codian VCR* web client.

15

Users, Connections and Notes

Users

RealPresence Collaboration Server Web Client Users are defined in the User's table and can connect to the MCU to perform various operations.

A maximum of 100 users can be defined per MCU.

User Types

The MCU supports the following user Authorization Levels:

- *Administrator*
- *Administrator Read-only*
- *Operator*
- *Chairperson*
- *Auditor*
- *Machine Account (Application-user)*

- *Chairperson* and *Auditor* user Authorization Levels are not supported in *Ultra Secure Mode*.
- Users with *Auditor* authorization level cannot connect to the RMX via the RMX Manager application and must use the RMX Web Client.

The authorization level determines a user's capabilities within the system.

Administrator

An administrator can define and delete other users, and perform all configuration and maintenance tasks.

Administrator Read-only

A user with Administrator permission with the same viewing and monitoring permissions of a regular Administrator. However, this user is limited to creating system backups and cannot perform any other configuration or conference related operation.

Operator

An Operator can manage Meeting Rooms, Profiles, Entry Queues, and SIP Factories, and can also view the RMX configurations, but cannot change them.

Administrator and Operator users can verify which users are defined in the system. Neither of them can view the user passwords, but an Administrator can change a password.

Chairperson

A Chairperson can only manage ongoing conferences and participants. The Chairperson does not have access to the RMX configurations and utilities.

Auditor

An **Auditor** can only view *Auditor Files* and audit the system.

Machine Account

User names can be associated with servers (machines) to ensure that all users are subject to the same account and password policies.

For enhanced security reasons it is necessary for the RMX to process user connection requests in the same manner, whether they be from regular users accessing the RMX via the *RMX Web Browser* / *RMX Manager* or from *application-users* representing applications such as *CMA* and *DMA*.

Regular users can connect from any workstation having a valid certificate while application-users representing applications can only connect from specific servers. This policy ensures that a regular user cannot impersonate an *application-user* to gain access to the RMX in order to initiate an attack that would result in a *Denial of Service* (*DoS*) to the impersonated application.

The connection process for an *application-user* connecting to the RMX is as follows:

1 The *application-user* sends a connection request, including its *TLS* certificate, to the RMX.

2 The RMX searches its records to find the *FQDN* that is associated with the *application-user's* name.

3 If the *FQDN* in the received certificate matches that associated with *application-user*, and the password is correct, the connection proceeds.

Guidelines

- *Application-users* are only supported when *TLS* security is enabled and *Request peer certificate* is selected. *TLS* security cannot be disabled until all *application-user* accounts have been deleted from the system.
- For *Secure Communications*, an administrator must set up on the RMX system a machine account for the *CMA* system with which it interacts. This machine account must include a fully-qualified domain name (*FQDN*) for the *CMA* system.
- *Application-user* names are the same as regular user names.
  Example: the *CMA* application could have an *application-user* name of `CMA1`.
- The *FQDN* can be used to associate all user types: *Administrator*, *Operator* with the *FQDN* of a server.
- Multiple *application-users* can be configured the same *FQDN* name if multiple applications are hosted on the same server
- If the system is downgraded the *application-user's FQDN* information is not deleted from the RMX's user records.
- A *System Flag,* **PASS_EXP_DAYS_MACHINE,** enables the administrator to change the password expiration period of *application-user's* independently of regular users. The default flag value is 365 days.

- The server hosting an *application-user* whose password is about to expire will receive a login response stating the number of days until the *application-user's* password expires. This is determined by the value of the **PASSWORD_EXPIRATION_WARNING_DAYS** *System Flag*. The earliest warning can be displayed 14 days before the password is due to expire and the latest warning can be displayed 7 days before passwords are due to expire. An *Active Alarm* is created stating the number of days before the password is due to expire.
- The **MIN_PWD_CHANGE_FREQUENCY_IN_DAYS** *System Flag* does not effect *application-user* accounts. Applications typically manage their own password change frequency.
- If an *application-user* identifies itself with an incorrect *FQDN*, its account will not be locked, however the event is written to the *Auditor Event File*.
- If an *application-user* identifies itself with a correct *FQDN* and an incorrect password, its account will be locked and the event written to the *Auditor Event File*.
- An *application-user* cannot be the last administrator in the system. The last administrator must be regular user.
- User names are not case sensitive.

Monitoring

- An *application-user* and its connection is represented by a specific icon.

Active Directory

- When working with *Active Directory*, *CMA* and *DMA* cannot be registered within *Active Directory* as regular users. *CMA* and *DMA application-users* must be manually.
- The only restriction is that TLS mode is enabled together with client certificate validation.
- if the above configuration are set off it will not be possible to add machine accounts.
- When setting the TLS mode off the system should check the existence of a machine account and block this operation until all machine accounts are removed.

Listing Users

The *Users* pane lists the currently defined users in the system and their authorization levels. The pane also enables the administrators to add and delete users.

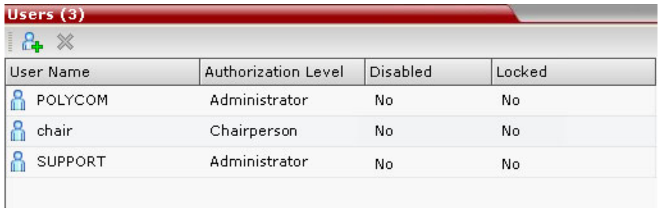
The system is shipped with a default Administrator user called POLYCOM, whose password is POLYCOM. However, once you have defined other authorized Administrator users, it is recommended to remove the default user.

You can view the list of users that are currently defined in the system.

To view the users currently defined in the system:

1 In the *RMX Management* pane, click the **Users** () button.

The *Users* pane is displayed.



The list includes three columns: User Name, Authorization Level and Disabled.

The *User Name* is the login name used by the user to connect to the MCU.

The *Authorization* indicates the Authorization Level assigned to the User: *Administrator, Administrator Read-only, Operator, Chairperson* or *Auditor*.

Disabled indicates whether the user is disabled and cannot access the system unless enabled by the administrator. For more details, see "*Disabling a User"* on page **15-6**.
Locked indicates whether the user has been locked out and cannot access the system unless enabled by the administrator.
In *Ultra Secure Mode* (ULTRA_SECURE_MODE=YES), Users can be automatically disabled or locked out by the system when they do not log into the RMX application for a predefined period or if their login session does not meet Enhanced Security requirements. Users can be manually disabled by the administrator. For more details, see "*User and Connection Management in Ultra Secure Mode"* on page **15-8**.

Adding a New User

Administrators can add new users to the system.

> The User Name and Password must be in ASCII.

To add a new user to the system:

1 In the *RMX Management* pane, click the **Users** ( ) button.

2 The *Users* pane is displayed.

3 Click the **New User** ( ) button or right-click anywhere in the pane and then click **New User**.

The *New User Properties* dialog box opens.

4. In the *User Name* text box, enter the name of the new user. This is the login name used by the user when logging into the system.
5. In the *Password* text box, enter the new user's password. This will be the user's password when logging into the system.
6. In the *Authorization Level* list, select the user type: **Administrator, Administator Read-Only, Operator, Chairperson** or **Auditor**.
7. **Optional. To associate a user with a machine**:
   a. In the *User Properties* dialog box, select the **Associate with a machine** check box.
   b. Enter the *FQDN* of the server that hosts the application who's application-user name is being added. Example: `cma1.polycom.com`
8. Click **OK**.
   The *User Properties* dialog box closes and the new user is added to the system.

Deleting a User

> To delete a user, you must have Administrator authorization. The last remaining Administrator in the *Users* list cannot be deleted.

1. In the *RMX Management* pane, click the **Users** ( ) button.
2. Select the user and click the **Delete** ( ) button or right-click the user and then click **Delete User**.

   The system displays a confirmation message.
3. In the *confirmation* dialog box, select **Yes** to confirm or **No** to cancel the operation.

   If you select **Yes**, the user name and icon are removed from the system.

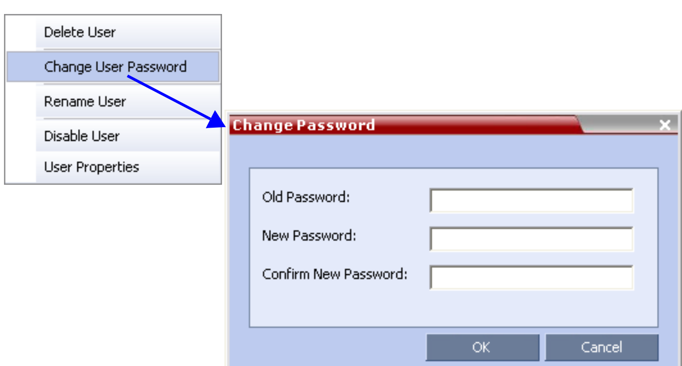
Changing a User's Password

Users with Administrator authorization can change their own password and other users' passwords. Users with Operator authorization can change their own password.

To change a user's password:

1. In the *RMX Management* pane, click the **Users** ( ) option.
2. Right-click the user and click **Change User Password**.

   The *Change Password* dialog box opens.



3 Enter the *Old Password* (current), *New Password* and *Confirm the New Password*.

The Password must be in ASCII.

4 Click **OK**.

The user's password is changed.

Disabling a User

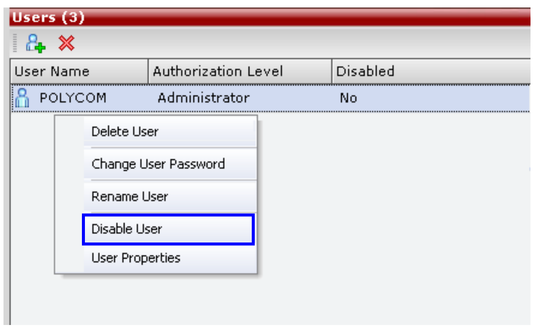
An administrator can disable an enabled user. An indication is displayed in the Users List when the User is disabled. An administrator can enable a disabled User.

To disable a user:

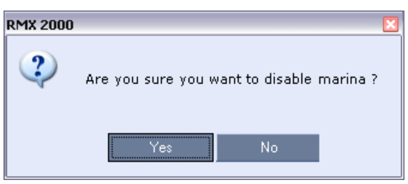
1 In the *RMX Management* pane, click the **Users** ( ) button.

The Users pane is displayed.

2 In the *Users* pane, right-click the user to be disabled and select **Disable User** in the menu.



A confirmation box is displayed.



3 Click **YES**.
The User status in the *Users* list - *Disabled* column changes to **Yes**.

Enabling a User

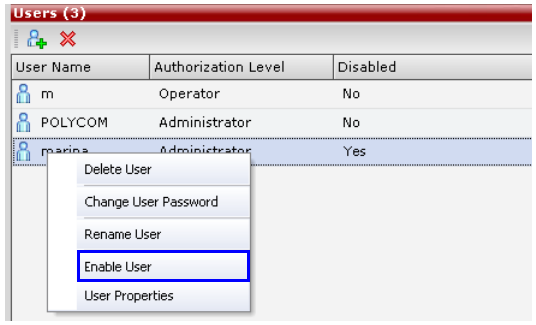
An administrator can enable a User who was disabled automatically by the system (in the *Ultra Secure Mode*) or manually by the administrator.

To enable a user:

1 In the *RMX Management* pane, click the **Users** ( ) button.

The *Users* pane is displayed.

2 Right-click the user to be enabled and select **Enable User**.



A confirmation box is displayed.

3 Click **YES**.
The User status in the *Users* list - *Disabled* column changes to **NO**.

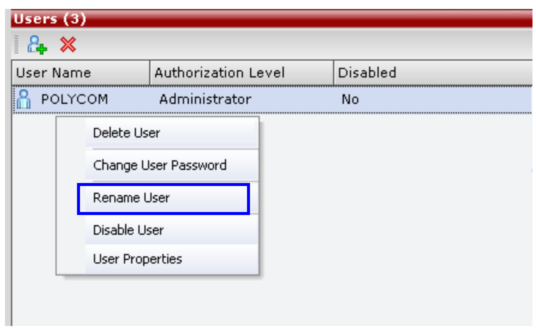
Renaming a User

To rename a user:

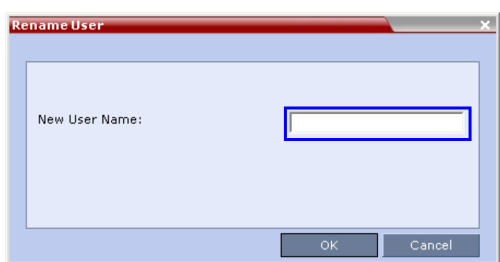
1 In the *RMX Management* pane, click the **Users** () button.

The Users pane is displayed.

2 Right-click the user to be renamed and select **Rename User**.



The *Rename User* dialog box is displayed.



3 Enter the user's new name in the *New User Name* field and click **OK**.

The user is renamed and is forced to change his/her password.

Connections

The RealPresence Collaboration Server enables you to list all connections that are currently logged into the MCU, e.g. users, servers or API users. The MCU issues an ID number for each login. The ID numbers are reset whenever the MCU is reset.

A maximum of 50 users can be concurrently logged in to the MCU.

Viewing the Connections List

To list the users who are currently connected to the MCU:

1 In the *RMX Management* pane, click the **Connections** ( ) button.
A list of connected users is displayed in the *Connections* pane.

Login Name	Authorization Level	Login Time	Workstation
POLYCOM	Administrator	9/20/2006 4:44 PM	EMA.F5-VARDAL-LT
POLYCOM	Administrator	9/20/2006 7:18 PM	EMA.F5-ZIVN
POLYCOM	Administrator	9/20/2006 10:46 AM	F3-NOAL

The information includes:

— The user's login name.
— The user's authorization level (Chairperson, Operator, Administrator or Auditor).
— The time the user logged in.
— The name/identification of the computer used for the user's connection.

User and Connection Management in Ultra Secure Mode

Additional security measures can be implemented in the RealPresence Collaboration Server by setting the appropriate system flags. These measures control the system users, the user connections to the MCU and the user login process.

Managing system users includes:

- User types that are not supported when the *Ultra Secure Mode* (ULTRA_SECURE_MODE=YES) is enabled.
- Disabling and enabling system Users.
- Renaming Users.
- Disabling inactive users.

Managing the user login process includes:

- Implementing Strong Passwords.
- Implementing password re-use / history rules.
- Defining password aging rules.
- Defining password change frequency.
- Forcing password change.
- Conference and Chairman Passwords.

- Locking out User.
- Displaying the User Login record.

Controlling the user sessions includes:

- Limiting the maximum number of concurrent user sessions.
- User session timeout.
- Limiting the maximum number of users that can connect to the system.

Managing the System Users

When the MCU is configured to *Ultra Secure Mode (*the **ULTRA_SECURE_MODE** *System Flag is set to* **YES)**, the following user management rules are automatically enforced:

User Types

- Auditor and chairperson user types are not supported.
- The *SUPPORT* user type is not allowed. If it exists, this user type is removed when the **ULTRA_SECURE_MODE** *System Flag is set to* **YES** and the system is restarted.

The *Audit* files can be retrieved by the Administrator User.

Disabling/Enabling Users

- An administrator can disable a user or enable a disabled user, including administrators.
- The last administrator cannot be disabled.

For more information see "*Disabling a User"* on page **15-6**.

Renaming Users

- An administrator can rename any user, including administrators.
- A renamed user is considered by the system to be a new user and is forced to change his/her password.

For more information see "*Renaming a User"* on page **15-7**.

Disabling Inactive Users

Users can be automatically disabled by the system when they do not log into the RMX application for a predefined period. When the RMX is configured to *Ultra Secure Mode (*the **ULTRA_SECURE_MODE** *System Flag is set to* **YES)**, this option is enforced.

- To enable this option, the **DISABLE_INACTIVE_USER** *System Flag* to a value between **1 to 90**. This value determines the number of consecutive days a user can be inactive before being disabled.

  When flag value is set to **0** (default in standard security environment), this option is disabled.

  The flag value is automatically set to **30** days when the **ULTRA_SECURE_MODE** *System Flag is set to* **YES.**
- The user is marked as disabled but is not deleted from the system administrator/ operator database.
- The user remains disabled until re-enabled by an administrator.
- If a disabled user attempts to *Login*, an error message, *Account is disabled*, is displayed.
- The last remaining administrator cannot be disabled.

For more information see "*Disabling a User"* on page **15-6**.

Managing the User Login Process

Implementing Strong Passwords

Strong Passwords can be implemented for logging into the RMX management applications. They can be implemented when the system is in standard security mode or when in *Ultra Secure Mode*.

The **FORCE_STRONG_PASSWORD_POLICY** *System Flag,* which enables or disables all password related flags cannot be set to **NO** and all *Strong Passwords* rules are automatically enabled and cannot be disabled when the **ULTRA_SECURE_MODE** *System Flag* is set to **YES**.

If an administrator modifies any of the *Strong Passwords* flag settings, all users are forced to perform the password change procedure, ensuring that all user passwords conform to the modified *Strong Passwords* settings.

Administrators can change passwords for users and other administrators. When changing passwords for him/herself, other administrators or other users, the administrator is required to enter his/her own administrator's password.

Strong Passwords rules are enforced according to the settings of the various *Strong Passwords* flags as described in Table 22-8, "*ULTRA_SECURE_MODE Flag Value – Effect on System Flags,*" on page **22-49**. Default settings of these flag change according to the system security mode.

Password Character Composition

- A *Strong Password* must contain **at least two** of **all** of the following character types:
  - — Upper case letters
  - — Lower case letters
  - — Numbers
  - — Special characters: @ # $ % ^ & * ( ) _ - = + | } { : " \ ] [; / ? > < , . (space) ~
- Passwords cannot contain the *User ID* (*User Name*) in any form. **Example:** A user with a *User ID*, *ben,* is not permitted to use "123**BeN**321" as a password because *BeN* is similar to the *User ID*.
- Passwords cannot contain more than four digits in succession.

When the strong password option is enabled and the password does not meet the Strong Password requirements an error, *Password characteristics do not comply with Enhance Security requirements,* is displayed.

Password Length

The length of passwords is determined by the value of the **MIN_PASSWORD_LENGTH** *System Flag*.

- Possible flag values are between 0 and 20.
- A *System Flag* value of **0** means this rule is not enforced, however this rule cannot be disabled when the RMX is in *Ultra Secure Mode*.
- In *Ultra Secure Mode,* passwords must be at least 15 characters in length (default) and can be up to 20 characters in length.
- If the *MIN_PASSWORD_LENGTH* flag is enabled and the password does not meet the required length an error, *Password is too short*, is displayed.

If the minimum password length is increased, valid pre-existing passwords remain valid until users are forced to change their passwords.

Implementing Password Re-Use / History Rules

Users are prevented from re-using previous passwords by keeping a list of previous passwords. If a password is recorded in the list, it cannot be re-used. The list is cyclic, with the most recently recorded password causing the deletion of the oldest recorded password.

- The number of passwords that are recorded is determined by the value of the **PASSWORD_HISTORY_SIZE** *System Flag*. Possible values are between 0 and 16.
- A flag value of **0** means the rule is not enforced, however this rule cannot be disabled when the RMX is in *Ultra Secure Mode*.
- In *Ultra Secure Mode,* at least 10 passwords (default) and up to 16 passwords must be retained.

If the password does not meet this requirement, an error, *New password was used recently*, is displayed.

Defining Password Aging

The duration of password validity is determined by the value of the **PASSWORD_EXPIRATION_DAYS** *System Flag*.

- Passwords can be set to be valid for durations of between 0 and 90 days.
- If the *System Flag* is set to **0**, user passwords do not expire. The *System Flag* cannot be set to **0** when the RMX is in *Ultra Secure Mode*.
- In *Ultra Secure Mode,* the minimum duration can be set to 7 days and the default duration is 60 days.

The display of a warning to the user of the number of days until password expiration is determined by the value of the **PASSWORD_EXPIRATION_WARNING_DAYS** *System Flag*.

- Possible number of days to display expiry warnings is between 0 and 14.
- If the *System Flag* is set to **0**, password expiry warnings are not displayed. The *System Flag* cannot be set to **0** when the RMX is in *Ultra Secure Mode*.
- In *Ultra Secure Mode,* the earliest warning can be displayed 14 days before passwords are due to expire and the latest warning can be displayed 7 days before passwords are due to expire (default setting).
- If a user attempts to log in after his/her password has expired, an error is displayed: *User must change password*.

Maximum Repeating Characters

A *System Flag* **MAX_PASSWORD_REPEATED_CHAR** allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a password.

Range: 1 - 4

Default: 2

A *System Flag* **MAX_CONF_PASSWORD_REPEATED_CHAR** allows the administrator to configure the maximum number of consecutive repeating characters that are to be allowed in a conference password.

Range: 1 - 4

Default: 2

Defining Password Change Frequency

The frequency with which a user can change a password is determined by the value of the **MIN_PWD_CHANGE_FREQUENCY_IN_DAYS** *System Flag*. The value of the flag is the number of days that users must retain a password.

- Possible retention period is between 0 and 7 days. In *Ultra Secure Mode* the retention period is between 1 (default) and 7.
- If the *System Flag* is set to **0**, users do not have to change their passwords. The *System Flag* cannot be set to **0** when the RMX is in *Ultra Secure Mode*.
- If a user attempts to change a password within the time period specified by this flag, an error, *Password change is not allowed before defined min time has passed*, is displayed.

An administrator can assign a new password to a user at any time.

Forcing Password Change

When the system is in *Ultra Secure Mode* the user is forced to change his/her password as follows:

- After modifying the value of the **ULTRA_SECURE_MODE** *System Flag* to **YES**, all RMX users are forced to change their *Login* passwords.
- When an administrator creates a new user, the user is forced to change his/her password on first *Login*.
- If an administrator changes a users *User ID* name, that user is forced to change his/her password on his/her next *Login*.
- If a user logs in using his/her old or default password, the *Login* attempt will fail. An error, *User must change password*, is displayed.
- Changes made by the administrator to any of the *Strong Password* enforcement *System Flags* render users' passwords invalid.

Example: A user is logged in with a fifteen character password. The administrator changes the value of the **MIN_PASSWORD_LENGTH** *System Flag* to **20**.
The next time the user tries to log in, he/she is forced to change his/her password to meet the updated *Strong Password* requirements.

Temporary User Lockout

When the **ULTRA_SECURE_MODE** *System Flag* is set to **YES,** *Temporary User Lockout* is implemented as a defense against *Denial of Service Attacks* or *Brutal Attacks.* Such attacks usually take the form of automated rapid *Login* attempts with the aim of gaining access to or rendering the target system (any network entity) unable to respond to users.

If a user tries to log in to the system and the *Login* is unsuccessful, the user's next *Login* attempt only receives a response from the RMX after 4 seconds.

User Lockout

User Lockout can be enabled to lock a user out of the system after three consecutive *Login* failures with same *User Name*. The user is disabled and only the administrator can enable the user within the system. User Lockout is enabled when the **USER_LOCKOUT** *System Flag* is set to **YES**.

If the user tries to login while the account is locked, an error message, *Account is disabled*, is displayed.

User Lockout is an *Audit Event*.

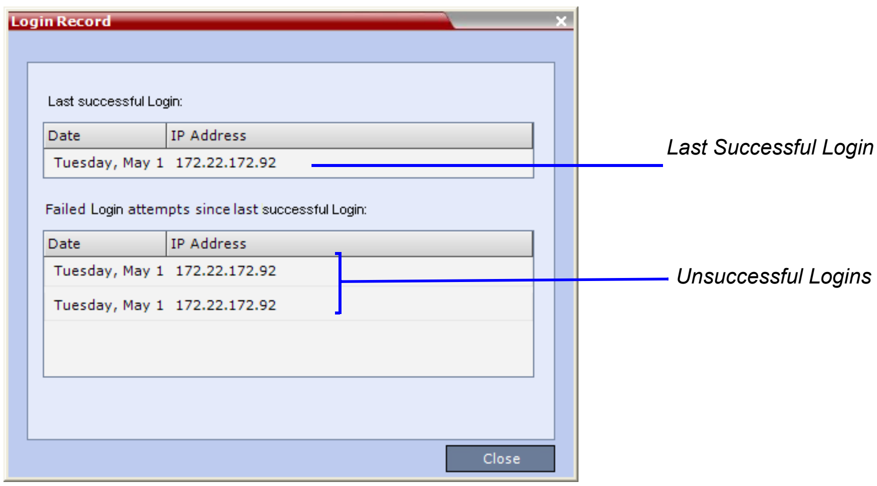
A system reset does not reset the *Login* attempts counter.

The time period during which the three consecutive *Login* failures occur is determined by the value of the **USER_LOCKOUT_WINDOW_IN_MINUTES** *System Flag*. A flag value of **0** means that three consecutive *Login* failures in any time period will result in *User Lockout*. Value can be between 0 and 45000.

The duration of the *Lockout* of the user is determined by the value of the **USER_LOCKOUT_DURATION_IN_MINUTES** *System Flag*. A flag value of **0** means permanent *User Lockout* until the administrator re-enables the user within the system. Value can be between 0 and 480.

User Login Record

The system can display a record of the last *Login* of the user. It is displayed in the *Main Screen* of the *RMX Web Client* or *RMX Manager*. The user *Login Record* display is enabled when the **LAST_LOGIN_ATTEMPTS** *System Flag* is set to **YES**.



Both lists display the:

- *Date* and *Time* of the *Login* attempt.
- *IP Address* of the workstation initiating the *Login* attempt.

The list of unsuccessful *Logins* can contain up to ten records.

Failed *Login* attempts are written to the system *Log Files* and are recorded as *Audit Events*. The *Audit* files can be retrieved by the Administrator User.

Controlling User Sessions

Management Sessions per System

It is possible for a several users to simultaneously log in to the RMX and initiate management sessions from different instances of the *RMX Web Client* or *RMX Manager* that are running on a single or several workstations.

The maximum number of concurrent management sessions (http and https connections) per system is determined by the value of the **MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM** *System Flag*.

Any attempt to exceed the maximum number of management sessions per system results in the display of an error message: *Maximum number of permitted user connections has been exceeded. New connection is denied.*

The log in attempt is recorded as an *Audit Event.*

Sessions per User

It is possible for a user to log in to the RMX and initiate multiple management sessions from different instances of the *RMX Web Client* or *RMX Manager* that are running on a single or several workstations.

The maximum number of concurrent management sessions per user (http and https connections) is determined by the value of the **MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER** *System Flag*.

Any attempt to exceed the maximum number of management sessions per user results in the display of an error message: *A user with this name is already logged into the system. Additional connection is denied.*

The log in attempt is recorded as an *Audit Event.*

Connection Timeout

If the connection is idle for longer than the number of seconds specified by the setting of the **APACHE_KEEP_ALIVE_TIMEOUT** *System Flag*, the connection to the RMX is terminated.

Session Timeout

If there is no input from the user or if the connection is idle for longer than the number of minutes specified by the setting of the **SESSION_TIMOUT_IN_MINUTES** *System Flag*, the connection to the MCU is terminated.

A flag value of **0** means *Session Timeout* is disabled, however this feature cannot be disabled when the MCU is in *Ultra Secure Mode*.

Erase Session History After Logout

In *Ultra Secure Mode,* the *RealPresence Collaboration Server Web Client* and RMX *Manager* leave no session information on the user's workstation or the MCU after the user logs off.

Notes

Notes are the electronic equivalent of paper sticky notes. You can use notes to write down questions, important phone numbers, names of contact persons, ideas, reminders, and anything you would write on note paper. *Notes* can be left open on the screen while you work.

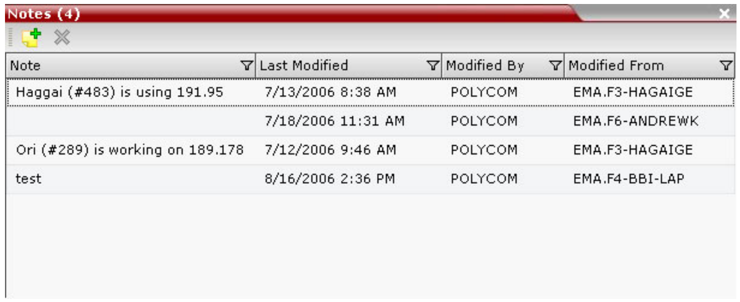
Notes can be read by all system Users concurrently connected to the MCU. Notes that are added to the *Notes* list are updated on all workstations by closing and re-opening the *Notes* window. Notes can be written in any Unicode language.

Using Notes

To create a note:

1 On the RealPresence Collaboration Server menu, click **Administration** > **Notes**.

The *Notes* window opens.



2 In the *Notes* toolbar, click the **New Note** ( ) button, or right-click anywhere inside the *Notes* window and select **New Note**.

3 In the *Note* dialog box, type the required text and click **OK**.

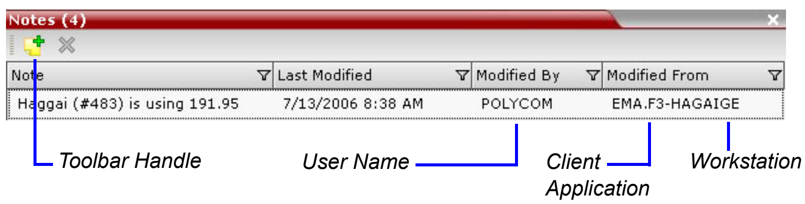
The new note is saved and closed. The *Notes* list is updated, listing the new note and its properties:

— **Note** – The beginning of the note's text.

— **Last Modified** – The date of creation or last modification.

— **Modified By** – The *Login Name* of the user who last modified the note.

— **Modified From** – The *Client Application* and *Workstation* from which the note was created or modified.



To open or edit a note:

4 Double-click the entry to edit, or right-click the entry and select **Note Properties**.

The note opens for viewing or editing.

To delete a note:

1 In the *Notes* list, select the entry for the note to delete and click the **Delete Note** button ( ), or right-click the entry and select **Delete Note**.

A *delete confirmation* dialog box is displayed.

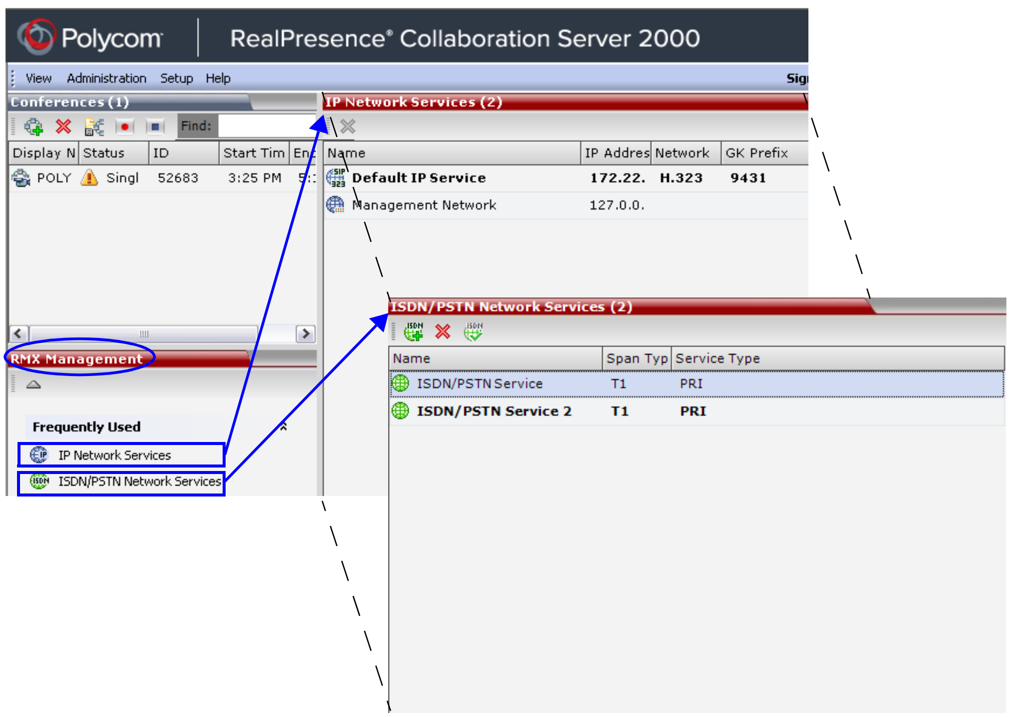
2 Click **OK** to delete the note, or click **Cancel** to keep the note.

16

Network Services

To enable the RealPresence Collaboration Server (RMX) to function within IP and ISDN/PSTN network environments, network parameters must be defined for both the *IP Network Services* and *ISDN/PSTN Network Services*. The IP Network Service must be defined for the RMX, while the ISDN/PSTN Network Service definition is optional and is done when the RTM ISDN cards are installed in the MCU.

The configuration dialog boxes for both these network services are accessed via the *RMX Management* pane of the *RealPresence Collaboration Server Web Client*.



IP Network Services

Two *IP Services* are defined for the RMX:

- **Management Network**
- **Default IP Service (Conferencing Service)**

Dial in, dial out connections and RMX management are supported within the following IP addressing environments:

- IPv6
- IPv4

- IPv6 & IPv4

When *IPv4* is selected, IPv6 fields are not displayed and conversely when *IPv6* is selected, *IPv4* fields are not displayed. When *IPv6 & IPv4* is selected both *IPv6* and *IPv4* fields are displayed.

For the purposes of comprehensive documentation, all screen captures in this chapter show the dialog boxes as displayed with *IPv6 & IPv4* selected.

For more information see "*Using IPv6 Networking Addresses for RMX Internal and External Entities*" on page **16-32**.

Management Network (Primary)

The *Management Network* is used to control the RMX, mainly via the *RealPresence Collaboration Server Web Client* application. The *Management Network* contains the network parameters, such as the IP address of the *Control Unit,* needed for connection between the RMX and the *RealPresence Collaboration Server Web Client.* This IP address can be used by the administrator or service personnel to connect to the *Control Unit* should the MCU become corrupted or inaccessible.

During *First Time Power-up*, the *Management Network* parameters can be set either via a *USB key* or by using a cable to create a private network.

For more information, see the*RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Modifying the Factory Default Management Network Settings on the USB Key*" on page **2-6** and *Appendix G* of this manual, "*Configuring Direct Connections to RealPresence Collaboration Server (RMX)*" on page **G-1**.

Default IP Service (Conferencing Service)

The *Default IP Service (Conferencing Service)* is used to configure and manage communications between the RMX and conferencing devices such as endpoints, gatekeepers, SIP servers, etc.

The *Default IP Service* contains parameters for:

- Signaling Host IP Address
- MPM, MPM+ and MPMx media cards (Media Processors
- External conferencing devices

Calls from all external IP entities are made to the *Signaling Host,* which initiates call set-up and assigns the call to the appropriate *MPM* / *MPM+* / *MPMx* media card.

> From *Version 7.1*, *MPM* media cards are not supported.

Conferencing related definitions such as environment (H.323 or SIP) are also defined in this service.

Most of the *Default IP Service* is configured by the *Fast Configuration Wizard,* which runs automatically should the following occur:

- First time power-up.
- Deletion of the D*efault IP Service*, followed by a system reset.

For more information, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "Procedure 1: First-time Power-up"* on page **2-25**.

Changes made to any of these parameters only take effect when the RMX is reset. An *Active Alarm* is created when changes made to the system have not yet been implemented and the MCU must be reset.

Modifying the Management Network

The *Management Network* parameters need to be modified if you want to:

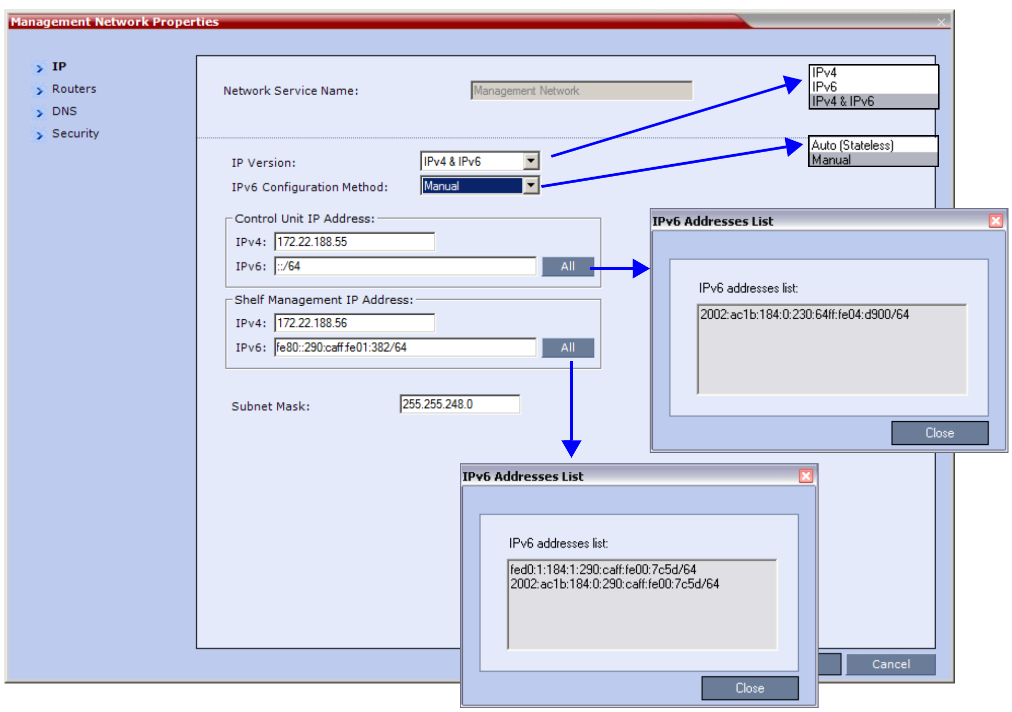
- Connect directly to the RMX from a workstation
- Modify routes
- Modify DNS information

To view or modify the Management Network Service:

1 In the *RMX Management* pane, click the **IP Network Services** ( ) button.

2 In the *IP Network Services* list pane, double-click the **Management Network** ( ) entry.

The *Management Network Properties - IP* dialog box opens.



On the RealPresence Collaboration Server (RMX) 2000 an additional tab called **LAN Ports** appears. For more information on the **LAN Ports** tab see Step 8.

3 Modify the following fields:

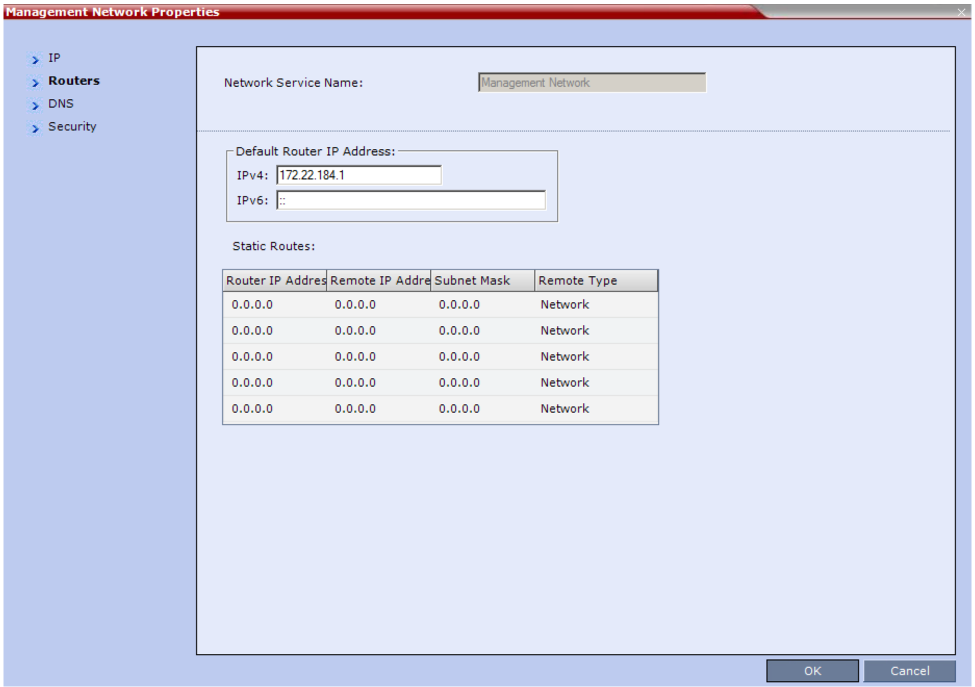
Table 16-1 *Default Management Network Service – IP*

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>Network Service Name</td><td colspan="2">Displays the name of the Management Network. This name cannot be modified.
Note: This field is displayed in all Management Network Properties tabs.</td></tr>
<tr><td rowspan="3">IP Version</td><td>IPv4</td><td>Select this option for IPv4 addressing only.</td></tr>
<tr><td>IPv6</td><td>Select this option for IPv6 addressing only.</td></tr>
<tr><td>IPv4 & IPv6</td><td>Select this option for both IPv4 and IPv6 addressing.
Note: If the gatekeeper cannot operate in IPv6 addressing mode, the H323_RAS_IPV6 System Flag should be set to NO.
For more information see Table 22-3, “Manually Added Flags - CS_MODULE_PARAMETERS Tab,” on page 22-39.</td></tr>
<tr><td rowspan="2">IPv6 Configuration Method</td><td>Auto (Stateless)</td><td>Select this option to allow automatic generation of the following addresses:
• Link-Local (For internal use only)
• Site-Local
• Global</td></tr>
<tr><td>Manual</td><td>Select his option to enable manual entry of the following addresses:
• Site-Local
• Global
Manual configuration of the following address types is not permitted:
• Link-Local
• Multicast
• Anycast</td></tr>
</table>

***Table 16-1** Default Management Network Service – IP (Continued)*

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td rowspan="3">Control Unit IP Address</td><td>IPv4</td><td colspan="2">The IPv4 address of the RMX. This IP address is used by the RealPresence Collaboration Server Web Client to connect to the RMX.</td></tr>
<tr><td rowspan="2">IPv6</td><td colspan="2">The IPv6 address of the MCU. This IP address is used by the RealPresence Collaboration Server Web Client to connect to the RMX.
Note: Internet Explorer 7™ is required for the RealPresence Collaboration Server Web Client to connect to the MCU using IPv6.</td></tr>
<tr><td>All</td><td>Click the All button to display the IPv6 addresses as follows:
• Auto - If selected, Site-Local and Global site addresses are displayed.
• Manual - If selected, only the Manual site address is displayed.</td></tr>
<tr><td rowspan="3">Shelf Management IP Address</td><td>IPv4</td><td colspan="2">The IPv4 address of the RMX Shelf Management Server. This IP address is used by the RealPresence Collaboration Server Web Client for Hardware Monitoring purposes.</td></tr>
<tr><td rowspan="2">IPv6</td><td colspan="2">The IPv6 address of the RMX Shelf Management Server. This IP address is used by the RealPresence Collaboration Server Web Client for Hardware Monitoring purposes.
Note: Internet Explorer 7™ is required for the RealPresence Collaboration Server Web Client to connect to the MCU using IPv6.</td></tr>
<tr><td>All</td><td>Click the All button to display the IPv6 addresses as follows:
• Auto - If selected, Site-Local and Global site addresses are displayed.
• Manual - If selected, only the Manual site address is displayed.</td></tr>
<tr><td>Subnet Mask</td><td colspan="3">Enter the subnet mask of the Control Unit.
Note: This field is specific to IPv4 and is not displayed in IPv6 only mode.</td></tr>
</table>

4 Click the **Routers** tab.



5 Modify the following fields:

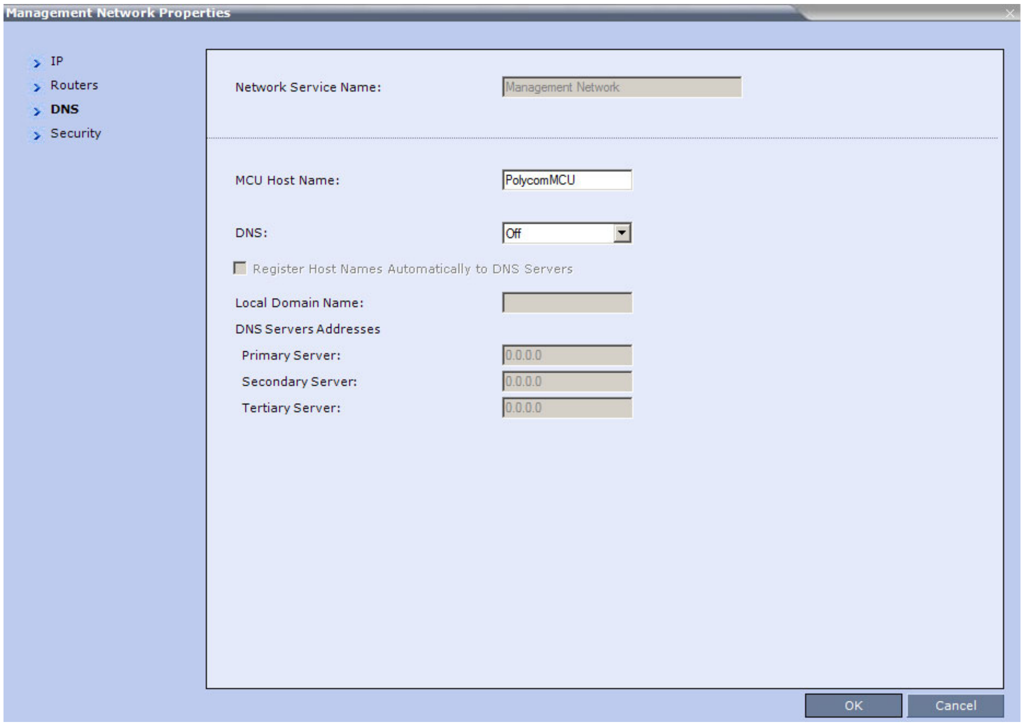
***Table 16-2** Default Management Network Service – Routers*

Field	Description	
Default Router IP Address	IPv4	Enter the IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.
	IPv6	

Table 16-2 *Default Management Network Service – Routers (Continued)*

Field	Description	
Static Routes IPv4 Only Table		The system uses *Static Routes* to search other networks for endpoint addresses that are not found on the local LAN. Up to five routers can be defined in addition to the Default Router. The order in which the routers appear in the list determines the order in which the system looks for the endpoints on the various networks. If the address is in the local subnet, no router is used. To define a static route (starting with the first), click the appropriate column and enter the required value.
	Router IP Address	Enter the IP address of the router.
	Remote IP Address	Enter the IP address of the entity to be reached outside the local network. The *Remote Type* determines whether this entity is a specific component (Host) or a network. • If Host is selected in the *Remote Type* field, enter the IP address of the endpoint. • If Network is selected in the *Remote Type* field, enter of the segment of the other network.
	Remote Subnet Mask	Enter the subnet mask of the remote network.
	Remote Type	Select the type of router connection: • **Network** – defines a connection to a router segment in another network. • **Host** – defines a direct connection to an endpoint found on another network.

6 Click the **DNS** tab.



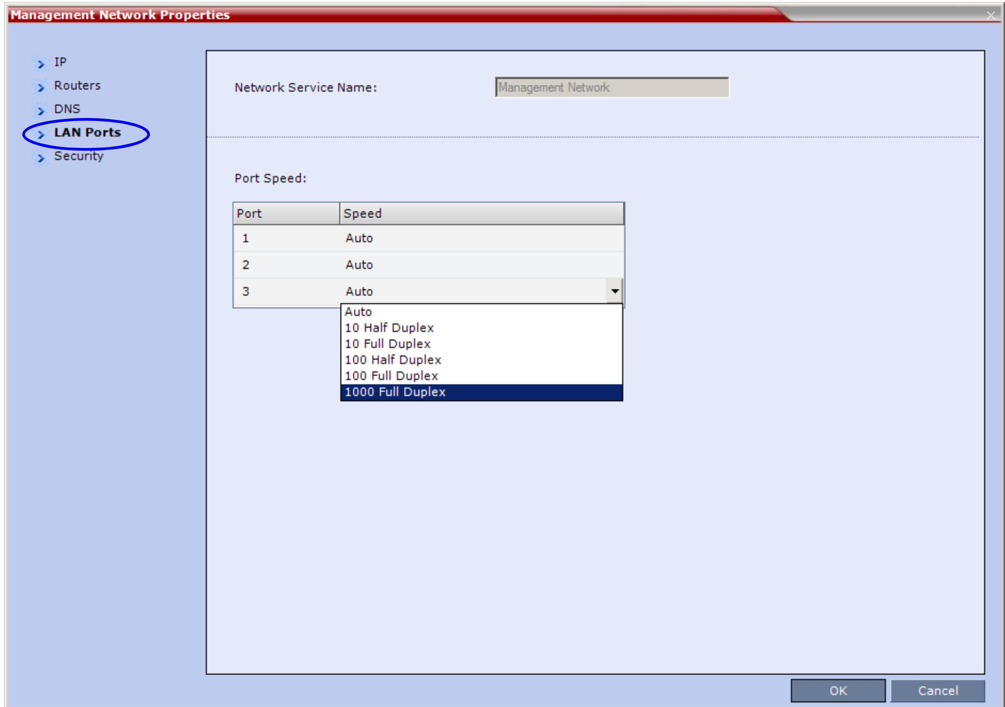
7 Modify the following fields:

***Table 16-3** Default Management Network Service – DNS*

Field	Description
MCU Host Name	Enter the name of the MCU on the network. Default name is RMX
DNS	Select: • **Off** – if DNS servers are not used in the network. • **Specify** – to enter the IP addresses of the DNS servers. **Note:** The IP address fields are enabled only if **Specify** is selected.
Register Host Names Automatically to DNS Servers	Select this option to automatically register the MCU Signaling Host and Shelf Management with the DNS server.
Local Domain Name	Enter the name of the domain where the MCU is installed.
DNS Servers Addresses:	
Primary Server	The static IP addresses of the DNS servers. A maximum of three servers can be defined.
Secondary Server	
Tertiary Server	

8 **RealPresence Collaboration Server (RMX) 2000 only:** Click the **LAN Ports** tab.

RMX 1500/4000 : If you want to modify the *LAN Port Speed Settings* on an RMX 1500/ 4000 see "*Ethernet Settings"* on page **16-24**.

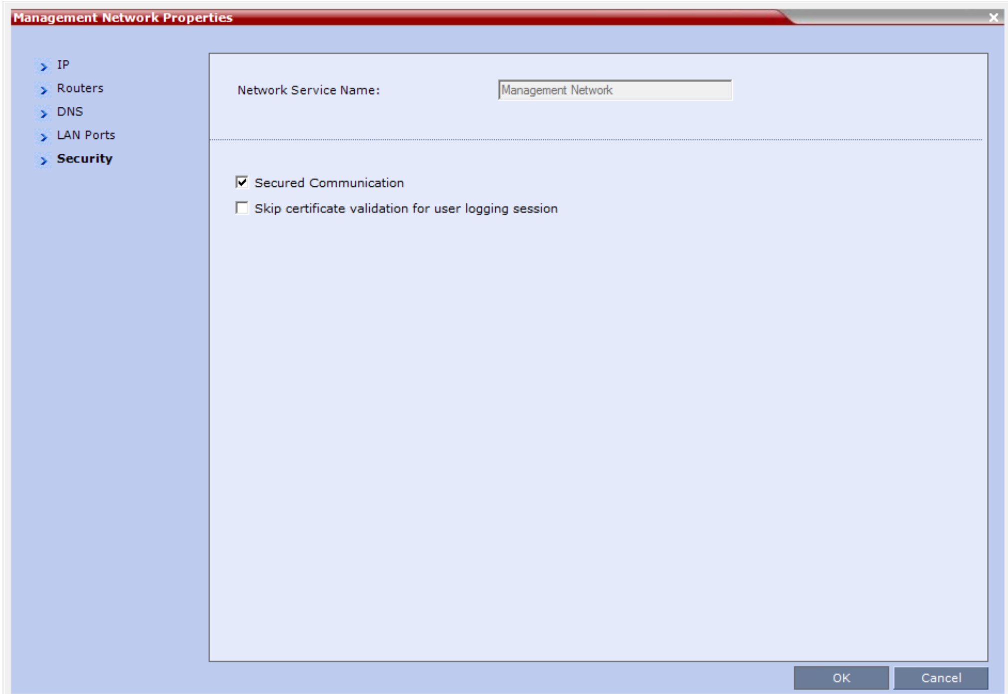


9 View or modify the following fields:

Table 16-4 *Management Network Properties – LAN Ports Parameters*

Field	Description	
Port Speed	The RealPresence Collaboration Server (RMX) 2000 has 3 LAN ports. The administrator can set the speed and transmit/receive mode manually for **LAN 2** Port only.	
	Port	The LAN port number: 1, 2 or 3. **Note:** Do not change the automatic setting of Port 1 and Port 3. Any change to Port 1 speed will not be applied.
	Speed	Select the speed and transmit/receive mode for each port. Default: Auto – Negotiation of speed and transmit/ receive mode starts at 1000 Mbits/second Full Duplex, proceeding downward to 10 Mbits/second Half Duplex. **Note:** To maximize conferencing performance, especially in high bit rate call environments, a 1Gb connection is recommended.

10 Click the **Security** tab.



11 Modify the following fields:

Table 16-5 Management Network Properties – Security Parameters

Field	Description
Secured Communication	Select to enable Secured Communication. The RMX supports TLS 1.0 and SSL 3.0 (Secure Socket Layer). A SSL/TLS Certificate must installed on the RMX for this feature to be enabled. For more information see "*Secure Communication Mode”* on page **F-1**.
Skip certificate validation for user logging session	Select this check box to prevent peer certificate requests being issued. For more information see "*(PKI) Public Key Infrastructure”* on page **F-8**. This check box must be cleared when enabling *Secured Mode*. If it is not cleared an *Active Alarm* is created and a message is displayed stating that *Secured Communications Mode* must be enabled.

12 Click **OK.**

13 If you have modified the *Management Network Properties*, reset the MCU.

Modifying the Default IP Network Service

The *Default IP Service* parameters need to be modified if you want to change the:

- Network type that the RMX connects to
- IP address of the RMX Signaling Host
- IP addresses of the RMX Media boards
- Subnet mask of the RMX's IP cards
- Gatekeeper parameters or add gatekeepers to the Alternate Gatekeepers list
- SIP server parameters

Fast Configuration Wizard

The *Fast Configuration Wizard* enables you to configure the *Default IP Service*. It starts automatically if no *Default IP Network Service* is defined. This happens during *First Time Power-up*, before the service has been defined or if the *Default IP Service* has been deleted, followed by an RMX restart.

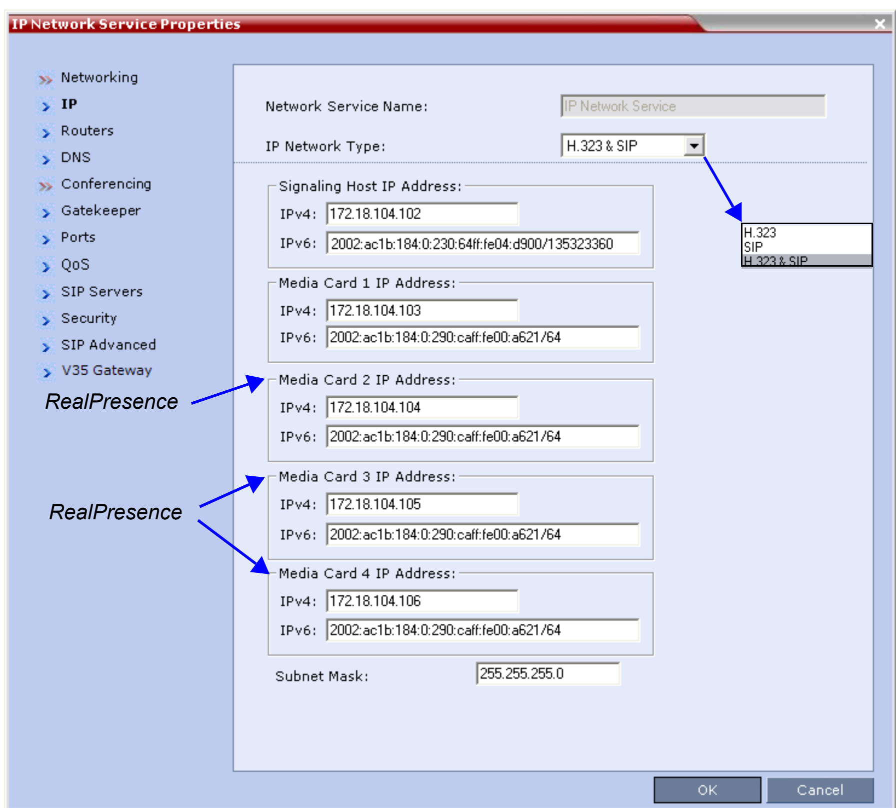
The *IP Management Service* tab in the *Fast Configuration Wizard* is enabled only if the factory default *Management IP addresses* were not modified.

If the *Fast Configuration Wizard* does not start automatically, the *Default IP Service* must be modified through the *IP Network Properties* dialog boxes.

To view or modify the Default IP Service:

1. In the *RMX Management* pane, click **IP Network Services** ( ).
2. In the *Network* list pane, double-click the **Default IP Service** (, , or) entry.

   The *Default IP Service - Networking IP* dialog box opens.

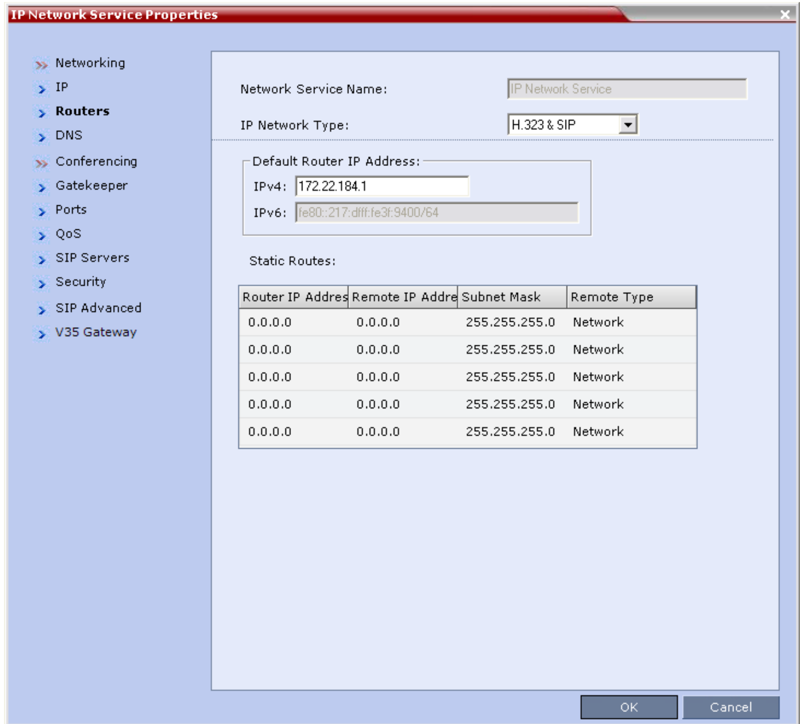


3 Modify the following fields:

Table 16-6 *Default IP Network Service – IP*

Field	Description
Network Service Name	The name *Default IP Service* is assigned to the IP Network Service by the Fast Configuration Wizard. This name can be changed. **Note:** This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.
IP Network Type	Displays the network type selected during the First Entry configuration. The Default IP Network icon indicates the selected environment. You can select: • **H.323:** For an H.323-only Network Service. • **SIP:** For a SIP-only Network Service. • **H.323 & SIP:** For an integrated IP Service. Both H.323 and SIP participants can connect to the MCU using this service. **Note:** This field is displayed in all Default IP Service tabs.
Signaling Host IP Address	Enter the address to be used by IP endpoints when dialing in to the MCU. Dial out calls from the RMX are initiated from this address. This address is used to register the RMX with a Gatekeeper or a SIP Proxy server.
Media Card 1 IP Address	Enter the IP address(es) of the media card (s) as provided by the network administrator: **RMX1500:** MPMx 1 **RMX 2000:** MPM/MPM+/MPMx 1 and MPM/MPM+/MPMx 2 (if installed) **RMX 4000:** MPM+/MPMx 1, MPM+/MPMx 2 (if installed), MPM+/MPMx 32 (if installed) and MPM+/MPMx 4 (if installed) Endpoints connect to conferences and transmit call media (video, voice and content) via these addresses.
Media Card 2 IP Address (RMX 2000/4000)	
Media Card 3 IP Address (RMX 4000)	
Media Card 4 IP Address (RMX 4000)	
Subnet Mask	Enter the subnet mask of the MCU. Default value: 255.255.255.0.

4 Click the **Routers** tab.



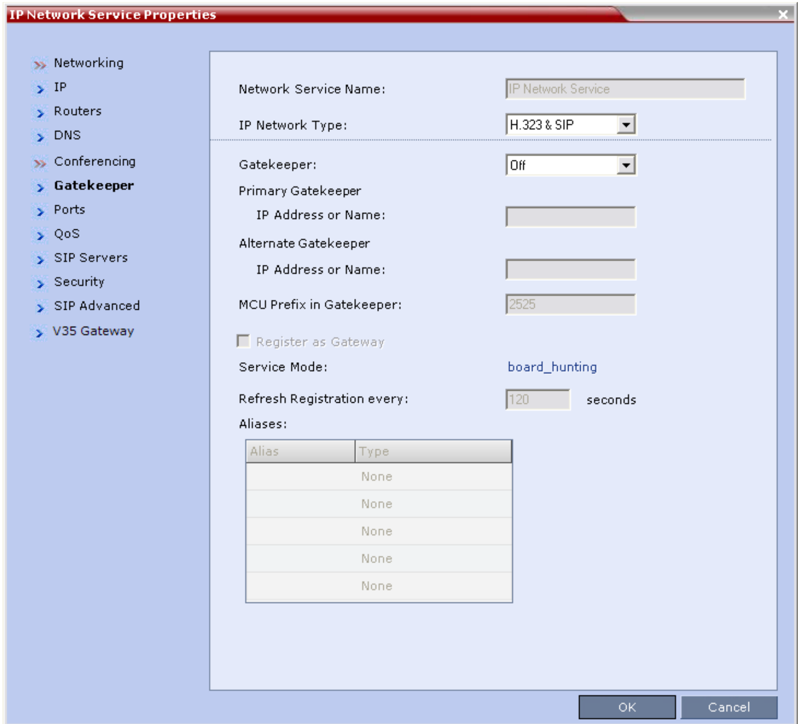
With the exception of *IP Network Type*, the field definitions of the *Routers* tab are the same as for the *Default Management Network*. For more information see "*Click the Routers tab."* on page **16-6**.

5 **Optional.** Click the **DNS** tab.

Settings in this dialog box are relevant to *Multiple Network Services* only.

For more information see "*Multiple Network Services"* on page **16-49**.

6 Click the **Gatekeeper** tab.



7 Modify the following fields:

***Table 16-7** Default IP Service – Conferencing – Gatekeeper Parameters*

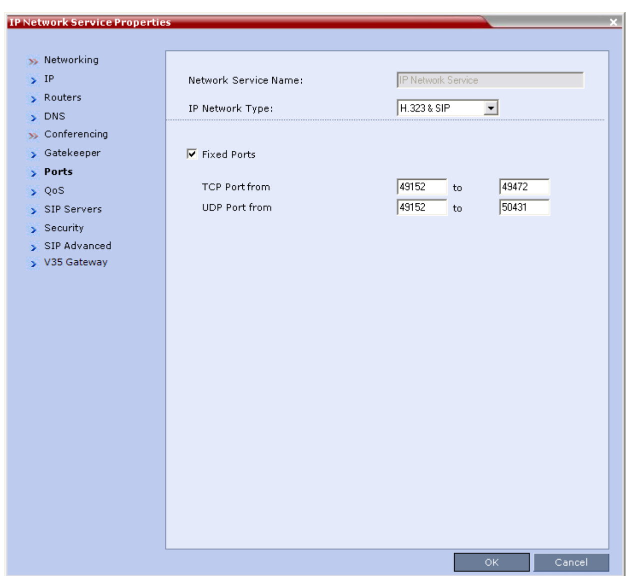
<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>Gatekeeper</td><td colspan="2">Select Specify to enable configuration of the gatekeeper IP address.
When Off is selected, all gatekeeper options are disabled.</td></tr>
<tr><td>Primary Gatekeeper IP Address or Name</td><td>Enter either the gatekeeper’s host name as registered in the DNS or IP address.</td><td rowspan="2">Note: When in IPv4&IPv6 or in IPv6 mode, it is easier to use Names instead of IP Addresses.</td></tr>
<tr><td>Alternate Gatekeeper IP Address or Name</td><td>Enter the DNS host name or IP address of the gatekeeper used as a fallback gatekeeper used when the primary gatekeeper is not functioning properly.</td></tr>
<tr><td>MCU Prefix in Gatekeeper</td><td colspan="2">Enter the number with which this Network Service registers in the gatekeeper. This number is used by H.323 endpoints as the first part of their dial-in string when dialing the MCU.
When PathNavigator or SE200 is used, this prefix automatically registers with the gatekeeper. When another gatekeeper is used, this prefix must also be defined in the gatekeeper.</td></tr>
<tr><td>Register as Gateway</td><td colspan="2">Select this check box if the RMX is to be seen as a gateway, for example, when using a Cisco gatekeeper.
Note: Do not select this check box when using Polycom ReadiManager/CMA 5000 or a Radvision gatekeeper.</td></tr>
</table>

Table 16-7 Default IP Service – Conferencing – Gatekeeper Parameters (Continued)

Field	Description
Refresh Registration every __ seconds	The frequency with which the system informs the gatekeeper that it is active by re-sending the IP address and aliases of the IP cards to the gatekeeper. If the IP card does not register within the defined time interval, the gatekeeper will not refer calls to this IP card until it re-registers. If set to 0, re-registration is disabled. **Note:** • It is recommended to use default settings. • This is a re-registration and not a 'keep alive' operation – an alternate gatekeeper address may be returned.
Aliases:	
Alias	The alias that identifies the RMX's Signaling Host within the network. Up to five aliases can be defined for each RMX. **Note:** When a gatekeeper is specified, at least one alias must be entered in the table. Additional aliases or prefixes may also be entered.
Type	The type defines the format in which the card's alias is sent to the gatekeeper. Each alias can be of a different type: • H.323 ID (alphanumeric ID) • E.164 (digits 0-9, * and #) • Email ID (email address format, e.g. abc@example.com) • Participant Number (digits 0-9, * and #) **Note:** Although all types are supported, the type of alias to be used depends on the gatekeeper's capabilities.

8 Click the **Ports** tab.

Settings in the *Ports* tab allow specific ports in the firewall to be allocated to multimedia conference calls.



The port range recommended by IANA (Internet Assigned Numbers Authority) is 49152 to 65535. The RMX uses this recommendation along with the number of licensed ports to calculate the port range.

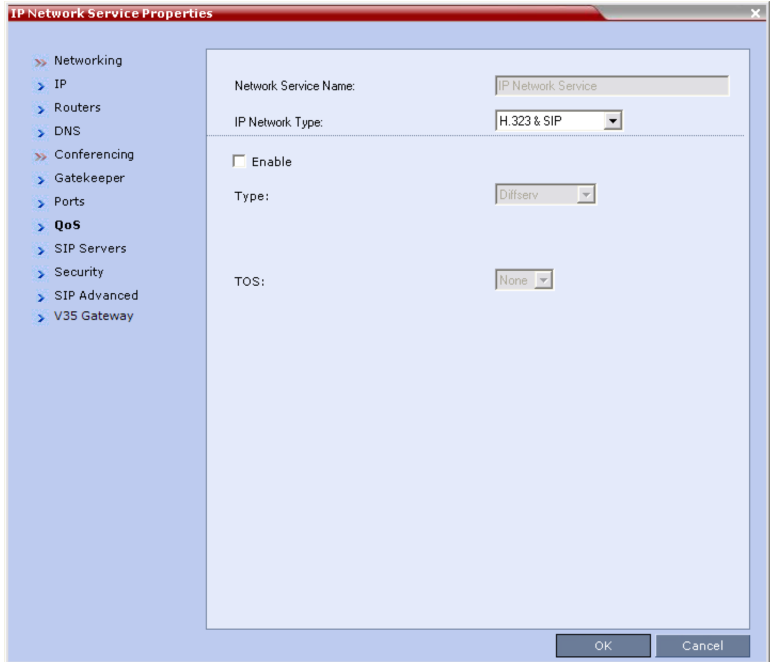
9 Modify the following fields:

Table 16-8 *Default IP Service – Conferencing – Ports Parameters*

Field	Description
Fixed Ports	Leave this check box cleared if you are defining a Network Service for local calls that do not require configuring the firewall to accept calls from external entities. When cleared, the system uses the default port range and allocates 4 RTP and 4 RTCP ports for media channels (Audio, Video, Content and FECC). **Note:** When ICE Environment is enabled, 8 additional ports are allocated to each call. Click this check box to manually define the port ranges or to limit the number of ports to be left open.
TCP Port from - to	Displays the default settings for port numbers used for signaling and control. To modify the number of TCP ports, enter the first and last port numbers in the range. The number of ports is calculated as follows: Number of simultaneous calls x 2 ports (1 signaling + 1 control).
UDP Port from - to	Displays the default settings for port numbers used for audio and video. To modify the number of UDP ports: • In *MPM Card Configuration Mode*: Enter the first and last port numbers in the range. The number of ports is calculated as follows: **Number of simultaneous calls x 8 ports** (2 audio, 2 video, 2 Content and 2 FECC). • In *MPM+/MPMx Card Configuration Mode*: Enter the first and last port numbers in the range, and the range must be **1024** ports. When ICE environment is enabled, the range must be **2048** ports.

If the network administrator does not specify an adequate port range, the system will accept the settings and issue a warning. Calls will be rejected when the RMX's ports are exceeded.

10 If required, click the **QoS** tab.



Quality of Service (QoS) is important when transmitting high bandwidth audio and video information. *QoS* can be measured and guaranteed in terms of:

- Average delay between packets
- Variation in delay (jitter)
- Transmission error rate

DiffServ and *Precedence* are the two *QoS* methods supported by the RMX. These methods differ in the way the packet's priority is encoded in the packet header.

The RMX's implementation of *QoS* is defined per Network Service, not per endpoint.

The routers must support QoS in order for IP packets to get higher priority.

11 View or modify the following fields:

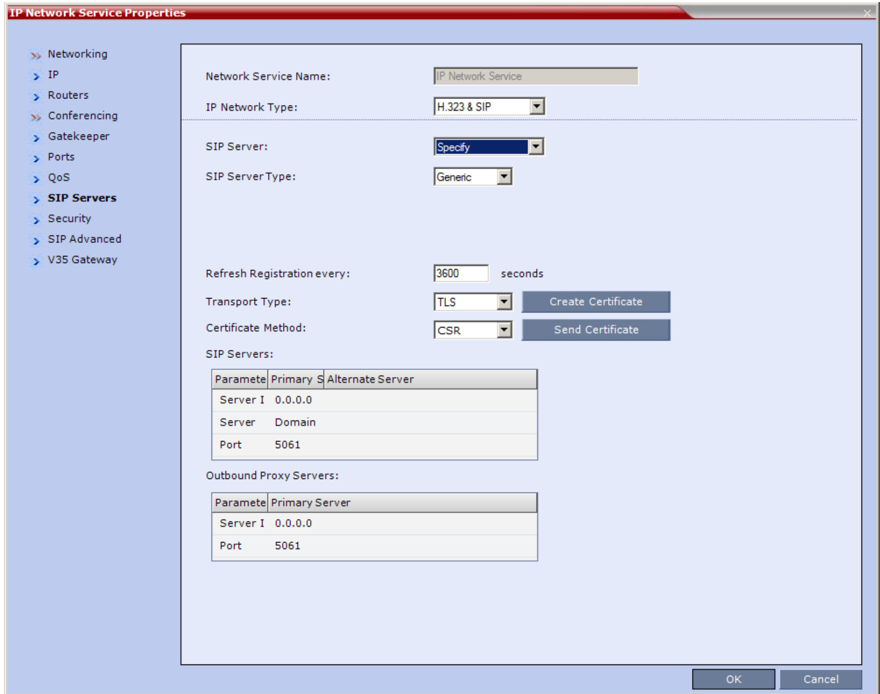
Table 16-9 *Default IP Service – Conferencing – QoS Parameters*

Field	Description
Enable	Select to enable the configuration and use of the QoS settings. When un-checked, the values of the DSCP (Differentiated Services Code Point) bits in the IP packet headers are zero.

Table 16-9 Default IP Service – Conferencing – QoS Parameters (Continued)

Field	Description
Type	DiffServ and Precedence are two methods for encoding packet priority. The priority set here for audio video and IP Signaling packets should match the priority set in the router. • **DiffServ:** Select when the network router uses DiffServ for priority encoding. The default priorities for both audio and video packets is 0x88. These values are determined by the QOS_IP_VIDEO and QOS_IP_AUDIO flags in the *system.cfg* file. The default priority for Signaling IP traffic is 0x00 and is determined by the QOS_IP_SIGNALING flag in the *system.cfg* file. For more information *"Modifying System Flags"* on page **22-1**. • **Precedence:** Select when the network router uses Precedence for priority encoding, or when you are not sure which method is used by the router. Precedence should be combined with None in the TOS field. The default priority is 5 for audio and 4 for video packets. **Note:** Precedence is the default mode as it is capable of providing priority services to all types of routers, as well as being currently the most common mechanism.
Audio / Video	You can prioritize audio and video IP packets to ensure that all participants in the conference hear and see each other clearly. Select the desired priority. The scale is from 0 to 5, where 0 is the lowest priority and 5 is the highest. The recommended priority is 4 for audio and 4 for video to ensure that the delay for both packet types is the same and that audio and video packets are synchronized and to ensure lip sync.
TOS	Select the type of Service (TOS) that defines optimization tagging for routing the conferences audio and video packets. • **Delay:** The recommended default for video conferencing; prioritized audio and video packets tagged with this definition are delivered with minimal delay (the throughput of IP packets minimizes the queue sequence and the delay between packets). • **None:** No optimization definition is applied. This is a compatibility mode in which routing is based on Precedence priority settings only. Select None if you do not know which standard your router supports.

12 Click the **SIP Servers** tab.



13 Modify the following fields:

Table 16-10 *Default IP Network Service – SIP Servers*

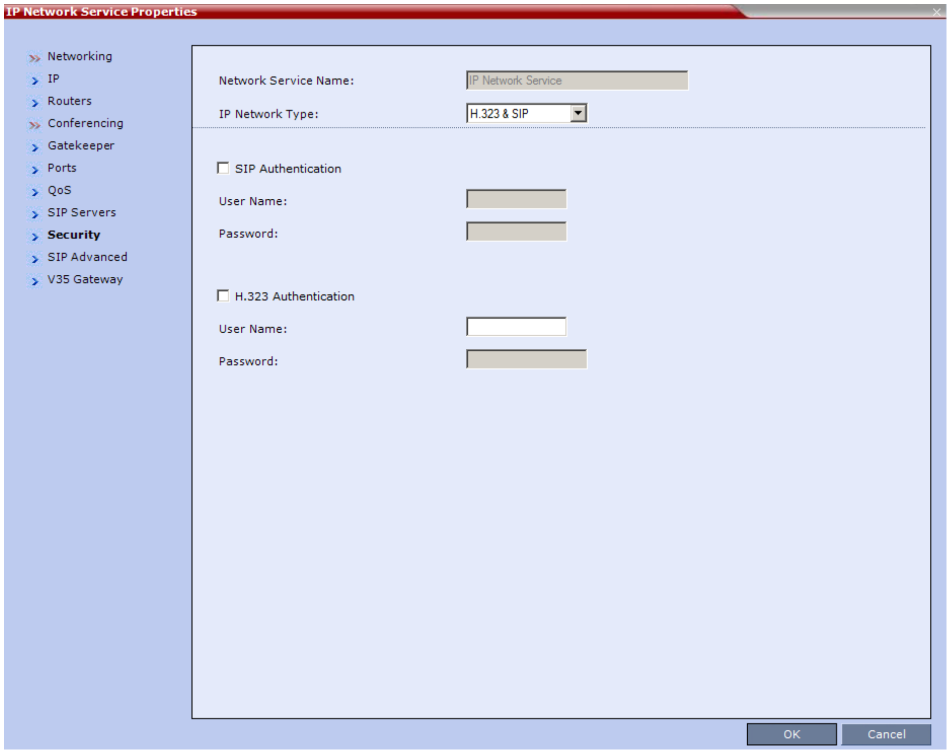
Field	Description
SIP Server	Select: • **Specify** – to manually configure SIP servers. • **Off** – if SIP servers are not present in the network.
SIP Server Type	Select: • Generic - for non Microsoft environments. • Microsoft - for Microsoft environments.
Refresh Registration	This defines the time in seconds, in which the RMX refreshes it's registration on the SIP server. For example, if "3600" is entered the RMX will refresh it's registration on the SIP server every 3600 seconds.
Transport Type	Select the protocol that is used for signaling between the RMX and the SIP Server or the endpoints according to the protocol supported by the SIP Server: **UDP –** Select this option to use UDP for signaling. **TCP –** Select this option to use TCP for signaling. **TLS –** The *Signaling Host* listens on secured port 5061 only and all outgoing connections are established on secured connections. Calls from SIP clients or servers to non secured ports are rejected. The following protocols are supported: TLS 1.0, SSL 2.0 and SSL 3.0.

***Table 16-10** Default IP Network Service – SIP Servers (Continued)*

Field	Description
Create Certificate	This button is used to create a Certificate Request to be sent to a Certification Authority.
Certificate Method	Select the method for sending the Certificate to the RMX: • CSR • PEM/PFX For more information see "*The Security Certificate"* on page **H-37**.
Send Certificate	This button is used when Integrating the RMX into the Microsoft OCS Environment. For more information, see "*Setting the MCU for Integration Into Microsoft Environment"* on page **H-1**.
SIP Servers: Primary / Alternate Server Parameter	
Server IP Address	Enter the IP address of the preferred SIP server. If a DNS is used, you can enter the SIP server name. **Note:** When in IPv4&IPv6 or in IPv6 mode, it is easier to use *Names* instead of *IP Addresses*.
Server Domain Name	Enter the name of the domain that you are using for conferences, for example: `user_name@domain name` The domain name is used for identifying the SIP server in the appropriate domain according to the host part in the dialed string. For example, when a call to `EQ1@polycom.com` reaches its outbound proxy, this proxy looks for the SIP server in the `polycom.com` domain, to which it will forward the call. When this call arrives at the SIP server in `polycom.com`, the server looks for the registered user (EQ1) and forwards the call to this Entry Queue or conference.
Port	Enter the number of the TCP or UDP port used for listening. The port number must match the port number configured in the SIP server. Default port is 5060.
Outbound Proxy Servers: Primary / Alternate Server Parameter	
Server IP Address	By default, the Outbound Proxy Server is the same as the SIP Server. If they differ, modify the IP address of the Outbound Proxy and the listening port number (if required). **Note:** When in IPv4&IPv6 or in IPv6 mode, it is easier to use *Names* instead of *IP Addresses*.
Port	Enter the port number the outbound proxy is listening to. The default port is 5060.

When updating the parameters of the SIP Server in the *IP Network Service - SIP Servers* dialog box, the RMX must be reset to implement the change.

14 Click the **Security** tab.



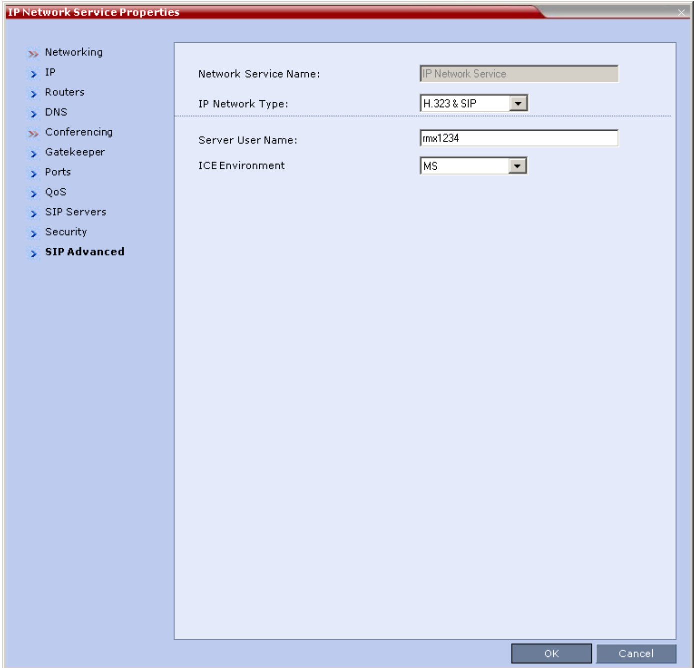
15 Modify the following fields:

***Table 16-11** Default IP Network Service – Security (SIP Digest)*

Field		Description	
SIP Authentication		Select to enable SIP server authentication.	These fields can contain up to 20 ASCII characters.
	User Name	Enter the conference, Entry Queue or Meeting Room name as registered with the proxy.	
	Password	Enter the conference, Entry Queue or Meeting Room password as defined with the proxy.	
H.323 Authentication		Select to enable H.323 server authentication.	
	User Name	Enter the conference, Entry Queue or Meeting Room name as registered with the proxy.	
	Password	Enter the conference, Entry Queue or Meeting Room password as defined with the proxy.	

If the *Authentication User Name* and *Authentication Password* fields are left empty, the SIP Digest authentication request is rejected. For registration without authentication, the RMX must be registered as a trusted entity on the SIP server.

16 **Optional.** To configure the ICE environment, click the **SIP Advanced** tab.



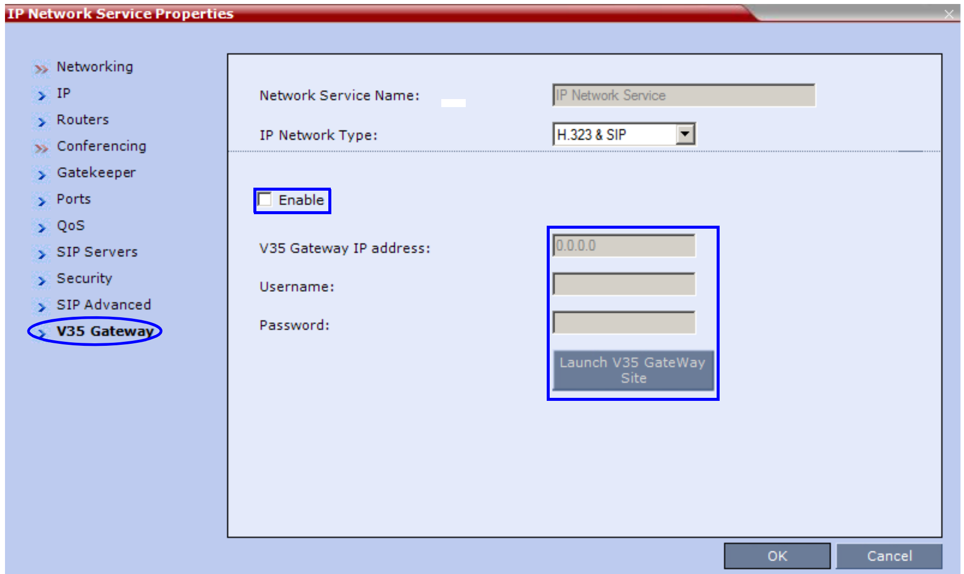
17 Modify the following fields:

Table 16-12 Default IP Network Service – SIP Advanced

Field	Description
Server User Name	Enter the *RMX User* name as defined in the *Active Directory*. For example, enter *rmx1234*. This field is disabled if the *ICE Environment* field is set to *None*.
ICE Environment	Select **MS** (for *Microsoft ICE* implementation) to enable the *ICE* integration. This field is disabled if the RMX is not running in *MPM+ Card Configuration Mode*.

18 **Optional.** Click the **V35 Gateway** tab.

The network service *Properties* dialog box is displayed.



19 Modify the following fields:

Table 16-13 *Network Service - V35 tab*

Field	Description
V35 Gateway IP Address	Enter the *Management IP* address of the management interface of the *Serial Gateway*. For more information see the *Polycom RealPresence Collaboration Server (RMX) 1500/2000/4000 Deployment Guide for Maximum Security Environments*, "*Deploying a Polycom RMX™ Serial Gateway S4GW"* on page **19-29**.
Username	Enter the *User Name* that the RMX uses to log in to the management interface of the Serial Gateway.
Password	Enter the *Password* that the RMX uses to log in to management interface of the *Serial Gateway*.

20 Click the **OK** button.

When updating the parameters of the SIP Server in the *IP Network Service - SIP Servers* dialog box, the RMX must be reset to implement the change.

Ethernet Settings

In the RMX 1500/4000 the automatically identified speed and transmit/receive mode of each LAN port used by the system can be manually modified if the specific switch requires it. These settings can be modified in the *Ethernet Settings* dialog box and they are not part of the *Management Network* dialog box as for the RealPresence Collaboration Server (RMX) 2000.

RealPresence Collaboration Server (RMX) 1500: The *Port* numbers displayed in the dialog box do not reflect the physical *Port* numbers as labeled on the RealPresence Collaboration Server (RMX) 1500.

Table 16-14 shows the physical mapping of *Port Type* to the physical label on the back panel of the RealPresence Collaboration Server (RMX) 1500.

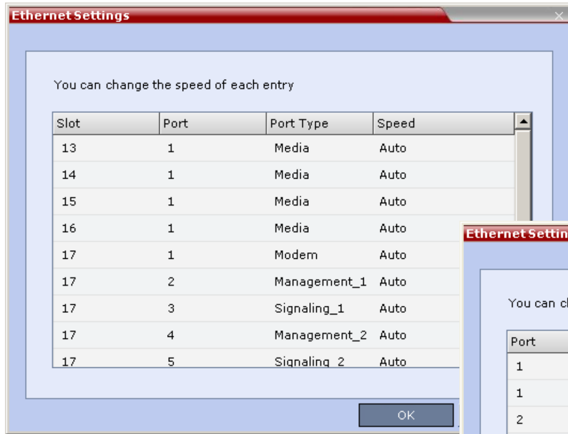
Table 16-14 *Physical Mapping - Port Type to Label on RealPresence Collaboration Server (RMX) 1500 and RealPresence Collaboration Server (RMX) 4000*

Port Type	Label on MCU		
	1500	4000	
Media	LAN 2	LAN 2	RTM LAN Card
Modem	Modem	LAN 1	RTM-IP 4000 Card
Management 1	MNG B	LAN 2	
Signaling 1	MNG	LAN 3	
ShM	Shelf	LAN 6	

To modify the automatic LAN port configuration:

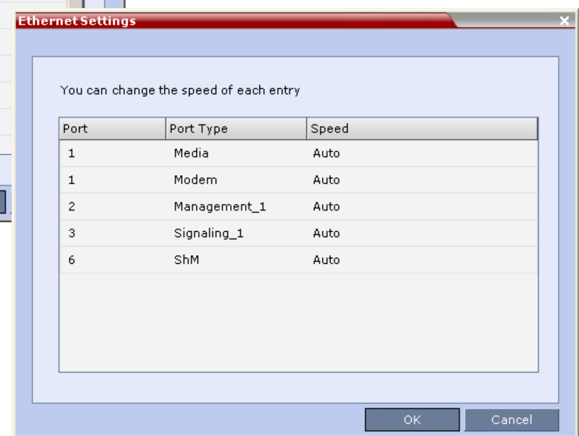
1 On the RMX menu, click **Setup > Ethernet Settings**.

The *Ethernet Settings* dialog box opens.



RealPresence Collaboration Server (RMX) 4000

RealPresence Collaboration Server (RMX) 1500



RMX 1500/4000 : Although the RTM LAN (media card) ports are shown as Port 1 in the *Ethernet Settings* and *Hardware Monitor*, the **physical LAN connection is Port 2.**

2 Modify the following field:

Table 16-15 *Ethernet Settings Parameters*

Field	Description	
Speed	The RMX has 3 LAN ports on the RTM-IP (Management, Signaling and Shelf Management), and additional LAN ports on each media card (RTM LAN) and RTM ISDN cards. The administrator can set the speed and transmit/receive mode manually for these ports.	
	Port	The LAN port number. **Note:** Do not change the automatic setting of Port 1,4 and Port 5 of the Management 2 and Signaling 2 Networks. Any change to the speed of these ports will not be applied.
	Speed	Select the speed and transmit/receive mode for each port. Default: Auto – Negotiation of speed and transmit/receive mode starts at 1000 Mbits/second Full Duplex, proceeding downward to 10 Mbits/second Half Duplex. **Note:** To maximize conferencing performance, especially in high bit rate call environments, a 1Gb connection is recommended. **Note:** **RealPresence Collaboration Server (RMX) 4000:** Do **not** select 1000 Full Duplex for any LAN ports in Slot 17. Select **only** 100 Full Duplex. **RealPresence Collaboration Server (RMX) 1500:** Do **not** select 1000 Full Duplex for Port 5 (ShM). Select **only** 100 Full Duplex.

3 Click the **OK** button.

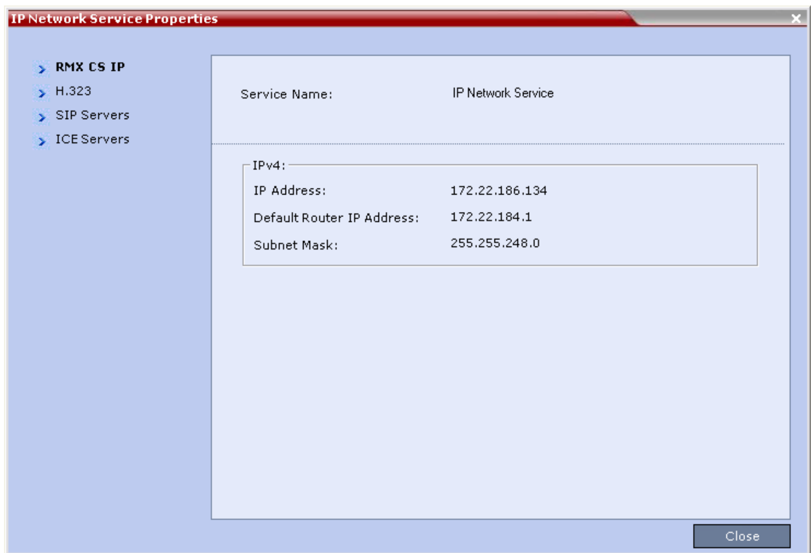
IP Network Monitoring

The *Signaling Monitor* is the RMX entity used for monitoring the status of external network entities such as the gatekeeper, DNS, SIP proxy and Outbound proxy and their interaction with the MCU.

To monitor signaling status:

1. In the *RMX Management* pane, click **Signaling Monitor** ( ).
2. In the *Signaling Monitor* pane, double-click **Default IP Service**.

   The *IP Network Services Properties – RMX CS IP* tab opens:



The *RMX CS IP* tab displays the following fields:

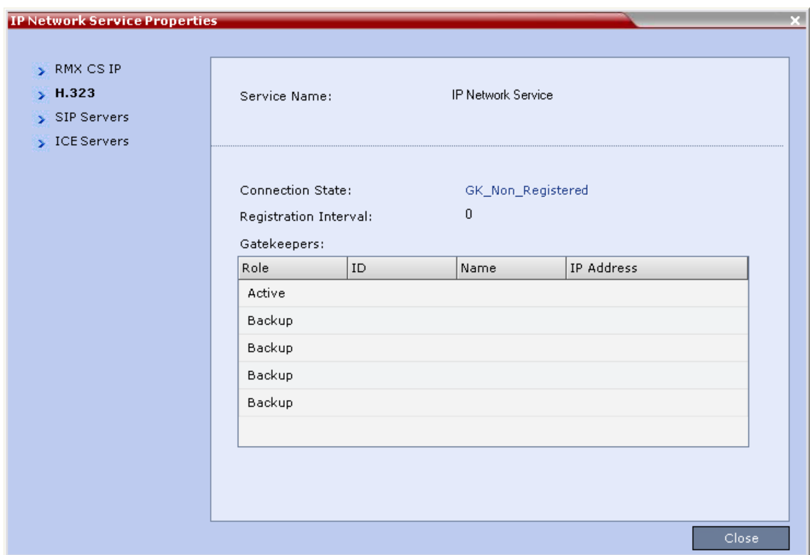
Table 16-16 *IP Network Services Properties – RMX CS IP*

Field	Description	
Service Name	The name assigned to the *IP Network Service* by the *Fast Configuration Wizard*. **Note:** This field is displayed in all tabs.	
IPv4	IP Address	
	Default Router IP Address	The IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.
	Subnet Mask	The subnet mask of the MCU. Default value: 255.255.255.0.

Table 16-16 *IP Network Services Properties – RMX CS IP (Continued)*

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td rowspan="4">IPv6</td><td rowspan="3">Scope</td><td colspan="2">IP Address</td></tr>
<tr><td>Global</td><td>The Global Unicast IP address of the RMX.</td></tr>
<tr><td>Site-Local</td><td>The IP address of the RMX within the local site or organization.</td></tr>
<tr><td>Default Router IP Address</td><td colspan="2">The IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.</td></tr>
</table>

3 Click the **H.323** tab.



The *H.323* tab displays the following fields:

Table 16-17 *IP Network Services Properties – H.323*

Field	Description
Connection State	The state of the connection between the Signaling Host and the gatekeeper: **Discovery** - The Signaling Host is attempting to locate the gatekeeper. **Registration** - The Signaling Host is in the process of registering with the gatekeeper. **Registered** - The Signaling Host is registered with the gatekeeper. **Not Registered** - The registration of the Signaling Host with the gatekeeper failed.

Table 16-17 *IP Network Services Properties – H.323 (Continued)*

Field	Description	
Registration Interval	The interval in seconds between the Signaling Host's registration messages to the gatekeeper. This value is taken from either the IP Network Service or from the gatekeeper during registration. The lesser value of the two is chosen.	
	Role	**Active** - The active gatekeeper. **Backup** - The backup gatekeeper that can be used if the connection to the preferred gatekeeper fails.
	ID	The gatekeeper ID retrieved from the gatekeeper during the registration process.
	Name	The gatekeeper's host's name.
	IP Address	The gatekeeper's IP address.

4 Click the **SIP Servers** tab.

The *SIP Servers* tab displays the following fields:

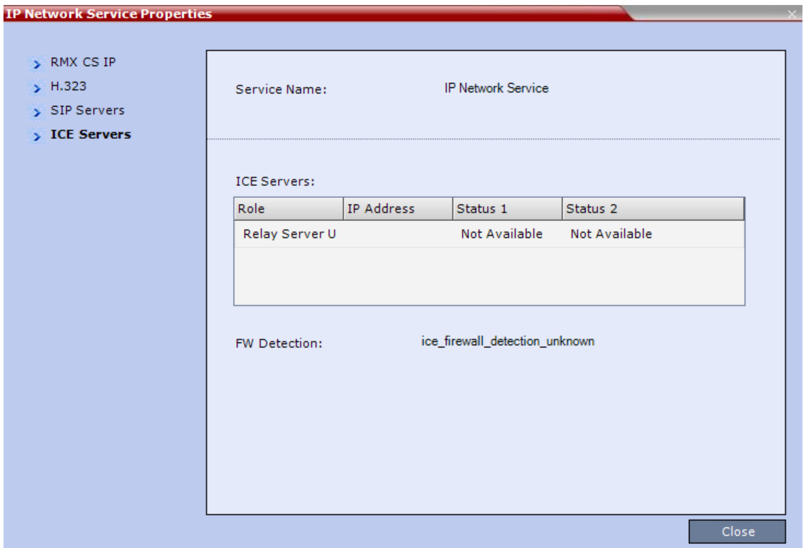
Table 16-18 *IP Network Services Properties – SIP Servers*

Field	Description
Role	**Active** -The default SIP Server is used for SIP traffic. **Backup** -The SIP Server is used for SIP traffic if the preferred proxy fails.
Name	The name of the SIP Server.
IP Address	The SIP Server's IP address.

Table 16-18 *IP Network Services Properties – SIP Servers (Continued)*

Field	Description
Status	The connection state between the SIP Server and the Signaling Host. **Not Available** - No SIP server is available. **Auto** - Gets information from DHCP, if used.

5 Click the **ICE Servers** tab.



The *ICE Servers* tab displays the following fields:

Table 16-19 *IP Network Services Properties – ICE Servers*

Field	Description
Role	The ICE Server's role is displayed: • STUN password server • STUN Server UDP • STUN Server TCP • Relay Server UDP • Relay Server TCP
IP Address	The ICE Server's IP Address.

Table 16-19 *IP Network Services Properties – ICE Servers (Continued)*

Field	Description
Status 1/2/3/4	A status is displayed for each media card installed in the RMX: • Connection O.K. • MS – register fail • MS – subscribe fail • MS – service fail • Connection failed • User/password failed • Channel didn't receive any packets for 5 seconds • Channel exceeded allotted bandwidth • Unknown failure In systems with multiple media cards, Status 1 refers to the uppermost media card.
FW Detection	The Firewall Detection status is displayed: • Unknown • UDP enabled • TCP enabled • Proxy -TCP is possible only through proxy • Block – both UDP & TCP blocked • None

Using IPv6 Networking Addresses for RMX Internal and External Entities

IPv6 addresses can be assigned to both *RMX* (*Internal*) and *External Entity* addresses.

RMX Internal Addresses

Default Management Network Service

- Control Unit
- Signaling Host
- Shelf Management
- MPM1 (Media Card)
- MPM2 (Media Card)

External Entities

- Gatekeepers (Primary & Secondary)
- SIP Proxies
- DNS Servers
- Default Router
- Defined participants

IPv6 Guidelines

- *Internet Explorer 7*™ is required for the *RealPresence Collaboration Server Web Client* and *RMX Manager* to connect to the RMX using *IPv6*.
- *IPv6* is supported with MPM+ and MPMx media cards only.
- The default IP address version is *IPv4*.
- The IP address field in the *Address Book* entry for a defined participant can be either *IPv4* or *IPv6*. A participant with an IPv4 address cannot be added to an ongoing conference while the RMX is in *IPv6* mode nor can a participant with an *IPv6* address be added while the RMX is in *IPv4* mode.

  An error message, *Bad IP address version,* is displayed and the *New Participant* dialog box remains open so that the participant’s address can be entered in the correct format.
- Participants that do not use the same IP address version as the RMX in ongoing conferences launched from *Meeting Rooms*, *Reservations* and *Conference Templates,* and are disconnected. An error message, *Bad IP address version,* is displayed.

  IP Security (IPSec) Protocols are not supported.

LAN Redundancy

LAN Redundancy enables the redundant LAN port connection to automatically replace the failed port by using another physical connection and NIC (Network Interface Card). When a LAN port fails, IP network traffic failure is averted and network or endpoints disconnections do not occur. When LAN cables are connected to both LAN 1 and LAN 2 ports, the RMX automatically selects which port is active and which is redundant.

Configuration Requirements

LAN Redundancy is available by default and is enabled by connecting the appropriate LAN cables to the LAN ports on the RMX as follows:

RealPresence Collaboration Server (RMX) 1500

- Connect the additional LAN cable to **LAN 1** port on the RTM IP.

RealPresence Collaboration Server (RMX) 2000

> On a RealPresence Collaboration Server (RMX) 2000, an *RTM LAN* card is required.
> For more information see the *RealPresence Collaboration Server (RMX) 2000 Hardware Guide*, "*Installing or Replacing the RTM LAN"* on page **1-37**.

- Connect the additional LAN cable to **LAN 1** port on the RTM LAN.
- **I**n the **Setup> System Configuration** > **System Flags** dialog box, add the flag **RMX2000_RTM_LAN** and set it to **YES** to activate the installed RTM LAN card.
- A system reset is required when adding the **RMX2000_RTM_LAN** flag.

RealPresence Collaboration Server (RMX) 4000

- Connect the additional LAN cable to **LAN 1** port on the RTM LAN.
- On the RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000, *LAN Redundancy* can be enabled simultaneously with *Multiple Networks*. To enable the *Multiple Networks* option, set the **MULTIPLE_SERVICES** flag to **YES**
- If required, reset the RMX.

On all systems:

- *LAN Redundancy* can be disabled by setting the **LAN_REDUNDANCY** *System Flag* to **NO**.
- If the **LAN_REDUNDANCY** *System Flag* value set to NO, the LAN 2 port must be connected to the IP network.

> On the RMX 1500/2000/4000, full media redundancy is supported if only one IP Network Service is defined per media card.

Media Redundancy

On the RealPresence Collaboration Server (RMX) 1500 LAN 1 and LAN 2 are the redundant media ports:

- LAN 2 port is used for standard communications

- LAN 1 port can be used to define a second Network Service or for LAN Redundancy

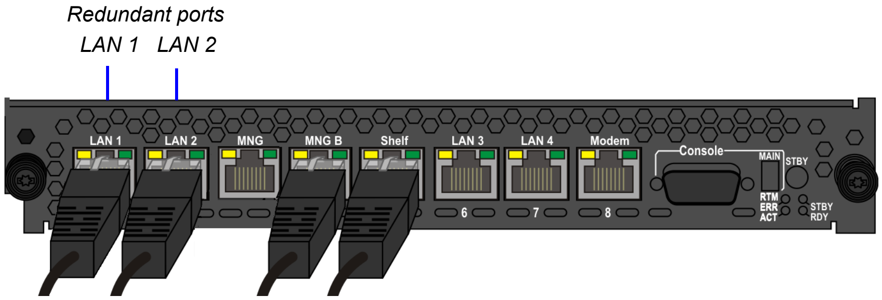


Figure 16-1 *RealPresence Collaboration Server (RMX) 1500 - RTM IP 1500 on Rear Panel*

On the RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000, the LAN 1 and LAN 2 port on the RTM LAN card can be used as redundant media ports.

Figure 16-2 *RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000 RTM LAN Card on Rear Panel*

Media Redundancy on the RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000 is dependent on the settings of the **LAN_REDUNDANCY** and **MULTIPLE_SERVICES** *System Flags* as summarized in Table 1-1

Table 16-20 *RMX 1500 / 2000 / 4000 - Media Redundancy - System Flags*

System Flag / Value	RMX 1500	RMX 2000	RMX 4000
LAN_REDUNDANCY = NO *MULTIPLE_SERVICES = NO*	No Redundancy		
LAN_REDUNDANCY = NO *MULTIPLE_SERVICES = YES*			
LAN_REDUNDANCY = YES *MULTIPLE_SERVICES = NO*	Full Redundancy	Media Redundancy Only	Full Redundancy
LAN_REDUNDANCY = YES *MULTIPLE_SERVICES = YES*	Full Media Redundancy (If only one *IP Network Service* is defined per media card.)		

Media Redundancy is not supported on any of the RMX RTM ISDN cards.

Signaling and Management Redundancy

RealPresence Collaboration Server (RMX) 1500

On the RealPresence Collaboration Server (RMX) 1500, for *Signaling* and *Management Redundancy*, the **MNG** port is redundant to the **MNG B** port and must have a LAN cable connected.

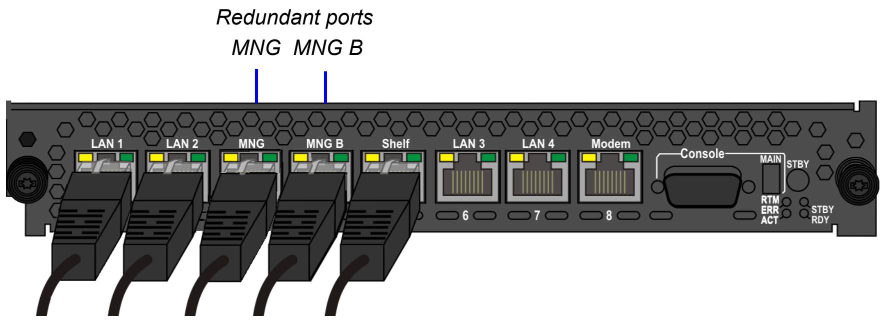


Figure 16-3 RealPresence Collaboration Server (RMX) 1500 - RTM IP 1500 on Rear Panel

RealPresence Collaboration Server (RMX) 4000

On the RealPresence Collaboration Server (RMX) 4000, for *Signaling* and *Management Redundancy* when LAN_REDUNDANCY = YES and MULTIPLE_SERVICES = NO, the **LAN 3** port on the *RTM-IP 4000* card is redundant to the **LAN 2** port.

LAN ports 4 and 5 are never used.

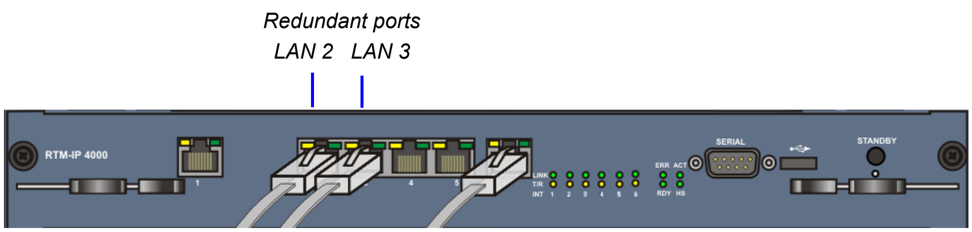


Figure 16-4 RealPresence Collaboration Server (RMX) 4000 - RTM IP 4000 on Rear Panel

On the RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 4000 *Signaling* and *Management Redundancy* is implemented using the LAN ports on the **RTM-IP** card and is dependent on the settings of the **LAN_REDUNDANCY** and **MULTIPLE_SERVICES** *System Flags* as summarized in Table 1-2

Table 16-21 *RMX 1500 / 4000 - Signaling and Management Redundancy - System Flags*

Flag / Value	Port Usage	
	LAN 2 / MNG B (RMX 1500)	**LAN 3 / MNG (RMX 1500)**
LAN_REDUNDANCY = NO *MULTIPLE_SERVICES = NO*	Management	Signaling
LAN_REDUNDANCY = NO *MULTIPLE_SERVICES = YES*	Management	Not Used
LAN_REDUNDANCY = YES *MULTIPLE_SERVICES = NO*	Management & Signaling (LAN3 is redundant to LAN 2)	

Table 16-21 *RMX 1500 / 4000 - Signaling and Management Redundancy - System Flags*

Flag / Value	Port Usage	
	LAN 2 / MNG B (RMX 1500)	**LAN 3 / MNG (RMX 1500)**
LAN_REDUNDANCY = YES *MULTIPLE_SERVICES = YES*	Management	Management

Hardware Monitor Indications

When LAN Redundancy is enabled on the RMX, LAN 2 port is *Active.* With LAN redundancy, when LAN LEDs are lit they indicate that a physical connection of the cables is present but does not indicate their activity status. In the *Hardware Monitor* pane the *Lan List* displays the RMX LAN ports together with their *Status* indication.

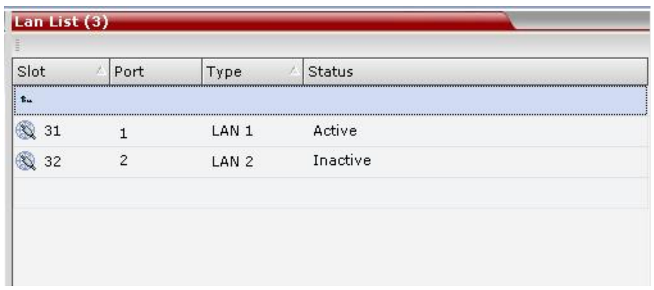


Table 16-22 *RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000 RTM LAN LED Indications*

Status	Description
Active	The LAN port cable is connected.
Inactive	The LAN port cable is not connected.
Standby	The LAN Redundancy option is enabled and this LAN port is the redundant and in standby mode. In case of failure, this port becomes active.

Network Traffic Control

A Network Traffic Control mechanism has been added to the RMX that controls the level of UDP packets generated by the system.

Only supported in the MPMx Card Configuration mode.

Network Traffic Control regulates a set of queuing systems and mechanisms by which UDP packets are received and "transmitted" to the network router. During a conference the MPMx cards occasionally blast-out UDP packets which can cause overloads on the network. RMX bandwidth usage can increase to above the designated conference participant line rate settings, causing network bandwidth issues such as latency and packet loss.

Three Network Traffic Control Flags are added:

- **ENABLE_TC_PACKAGE**
  When the flag is set to NO (default), Network Traffic Control is disabled on the RMX. Set the flag to YES to enable Network Traffic Control.
- **TC_BURST_SIZE**
  This flag regulates the Traffic Control buffer or maxburst size as a percentage of the participant line rate. In general, higher traffic rates require a larger buffer. For example, if the flag is set to 10 and the participants line rate is 2MB, then the burst size is 200Kbps.
  Default = 10
  Flag range: 1-30.
- **TC_LATENCY_SIZE**
  This flag limits the latency (in milliseconds) or the number of bytes that can be present in a queue.
  Default = 500
  Flag range: 1-1000 (in milliseconds).

SIP Proxy Failover With Polycom® Distributed Media Application™ (DMA™) 7000

RMX systems that are part of a *DMA* environment can benefit from *DMA*'s *SIP Proxy Failover* functionality.

SIP Proxy Failover is supported in DMA's *Local Clustering* mode with redundancy achieved by configuring two *DMA* servers to share a single virtual *IP* address.

The virtual *IP* address is used by the RMX as the *IP* address of its *SIP Proxy*.

No additional configuration is needed on the RMX.

Should a SIP Proxy failure occur in one of the DMA servers:

- The other *DMA* server takes over as *SIP Proxy*.
- Ongoing calls may be disconnected.
- Previously ongoing calls will have to be re-connected using the original *IP* address, registration and connection parameters.
- New calls will connect using the original *IP* address, registration and connection parameters.

RealPresence Collaboration Server (RMX) Network Port Usage

The following table summarizes the port numbers and their usage in the Polycom RealPresence Collaboration Server (RMX) 1500/2000/4000:

Table 16-23 *RMX Network Port Usage Summary*

Connection Type	Port Number	Protocol	Description	Configurable
HTTP	80	TCP	Management between the RMX and *RealPresence Collaboration Server Web Client*.	No
HTTPS	443	TCP	Secured Management between the RMX and *RealPresence Collaboration Server Web Client*.	No
DNS	53	TCP	Domain name server.	Can be disabled in the IP Network Service.
DHCP	68	TCP	Dynamic Host Configuration Protocol.	Can be disabled in the IP Network Service.
SSH	22	TCP	Secured shell. It is the RMX terminal.	No
NTP	123	UDP	Network Time Protocol. Enables access to a time server on the network.	No
H.323 GK RAS	1719	UDP	Gatekeeper RAS messages traffic.	No
H.323 Q.931	1720 - incoming ; 49152-59999 - outgoing	TCP	H.323 Q.931 call signaling. Each outgoing call has a separate port. The port for each outgoing call is allocated dynamically.	Yes - for outgoing calls only. It is configured in the Fixed Ports section of the IP service.
H.323 H.245	49152 - 59999	TCP	H.245 control. Each outgoing call has a separate port. The port for each outgoing call is allocated dynamically. It can be avoided by tunneling.	Yes - for outgoing calls only. It is configured in the Fixed Ports section of the IP service.
SIP server	5060 60000	UDP, TCP	Connection to the SIP Server. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.

Table 16-23 *RMX Network Port Usage Summary (Continued)*

Connection Type	Port Number	Protocol	Description	Configurable
Alternative SIP server	5060 60000	UDP, TCP	Connection to the alternate SIP Server. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
SIP Outbound proxy	5060 60000	UDP, TCP	Connection to the SIP outbound proxy. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
Alternative SIP Outbound proxy	5060 60000	UDP, TCP	Connection to the alternate SIP outbound proxy. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
SIP-TLS	60002	TCP	Required for Binary Floor Control Protocol (BFCP) functionality for SIP People+Content content sharing.	No - ,port is not opened if SIP People+Content is disabled.
RTP	49152 - 59999	UDP	RTP media packets. The ports are dynamically allocated.	Yes - It is configured in the Fixed Ports section of the IP service.
RTCP	49152 - 59999	UDP	RTP control. The ports are dynamically allocated.	Yes - It is configured in the Fixed Ports section of the IP service.
SIP -TLS	5061	TCP	SIP -TLS for SIP server, alternate SIP server, outbound proxy and alternate outbound proxy.	No

ISDN/PSTN Network Services

To enable ISDN and PSTN participants to connect to the MCU, an ISDN/PSTN Network Service must be defined. A maximum of two ISDN/PSTN Network Services, of the same *Span Type* (E1 or T1) can be defined for the RMX. Each Network Service can attach spans from either or both cards.

Most of the parameters of the first *ISDN/PSTN Network Service* are configured in the *Fast Configuration Wizard,* which runs automatically if an RTM ISDN card is detected in the RMX during first time power-up. For more information, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "First Entry Power-up and Configuration"* on page **2-25**.

Supported Capabilities and Conferencing Features:

- ISDN video is supported only in *Continuous Presence* (CP) conferences.
- Only BONDING (using multiple channels as a single, large bandwidth channel) is supported.
- Simple audio negotiation.
- Supported video resolutions are the same as for IP.
- Supported video Protocols are the same as for IP: H.261, H.263, H.264.
- H.239 for content sharing.
- Lecture Mode.
- DTMF codes.
- Securing of conferences.
- Basic cascading between two MCUs using an ISDN link is available and forwarding of DTMF codes can be suppressed.

Non Supported Capabilities and Conferencing Features:

- NFAS (Non-Facility Associated Signaling)
- Leased line usage
- Restricted Channel mode
- Aggregation of channels
- V.35 serial standards
- Primary and secondary clock source configuration (they are automatically selected by the system)
- Auto detection of *Audio Only* setting at endpoint
- Auto re-negotiation of bit rate
- Additional network services (two currently supported)
- Change of video mode (capabilities) from remote side during call
- Audio algorithms G.729 and G.723.1
- FECC
- H.243 Chair Control
- T.120 data sharing protocol
- H.261 Annex D
- MIH Cascading using an ISDN connection as cascade link

Adding/Modifying ISDN/PSTN Network Services

The system administrator can use the *RMX Management – ISDN/PSTN Network Services* section of the *RealPresence Collaboration Server Web Client* to add a second ISDN/PSTN Network Service or modify the first ISDN/PSTN Network Service.

A new ISDN/PSTN Network Service can be defined even if no RTM ISDN card is installed in the system.

Obtaining ISDN/PSTN required information

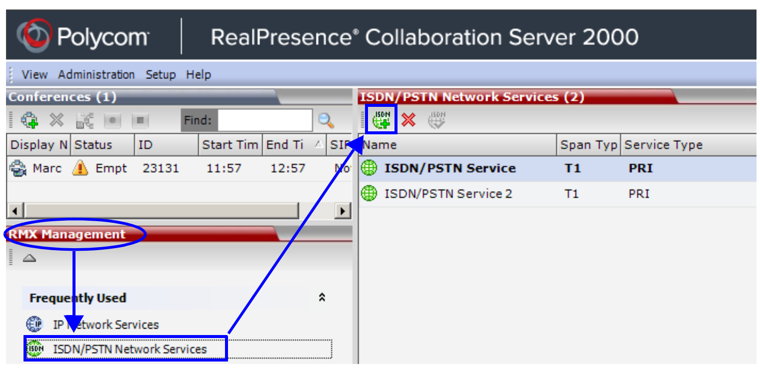
Before configuring the ISDN/PSTN Network Service, obtain the following information from your ISDN/PSTN Service Provider:

- Switch Type
- Line Coding and Framing
- Numbering Plan
- Numbering Type
- Dial-in number range

If the RMX is connected to the public ISDN Network, an external CSU or similar equipment is needed.

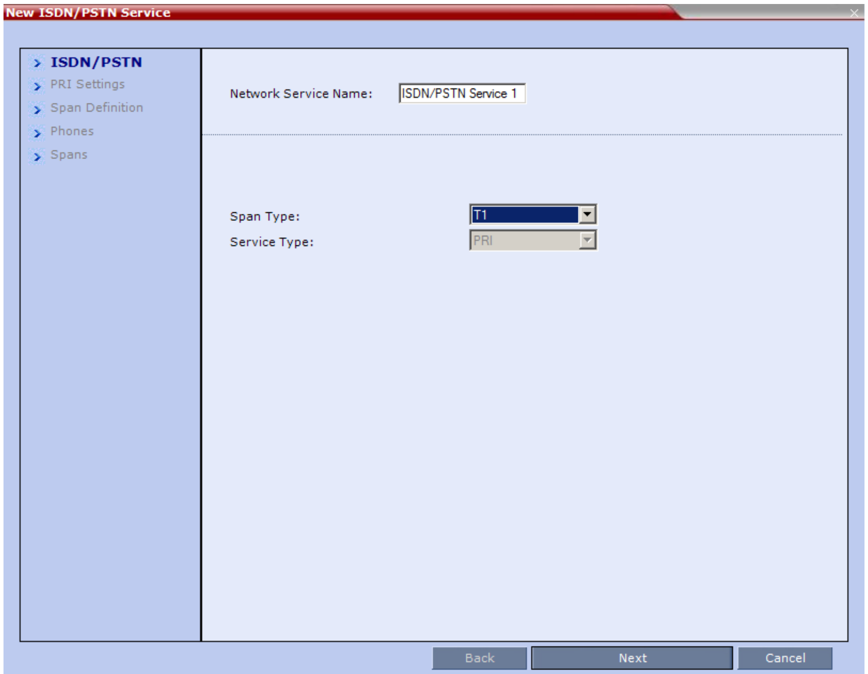
To Add an ISDN/PSTN Network Service:

1 In the *RMX Management pane*, click **ISDN/PSTN Network Services** ( ).



2 In the *ISDN/PSTN Network Services* list menu, click the **New ISDN/PSTN Service** button ( ) or right-click anywhere in the *ISDN/PSTN Network Services* list and select **New ISDN/PSTN Service**.

The *Fast Configuration Wizard* sequence begins with the *ISDN/PSTN* dialog box:



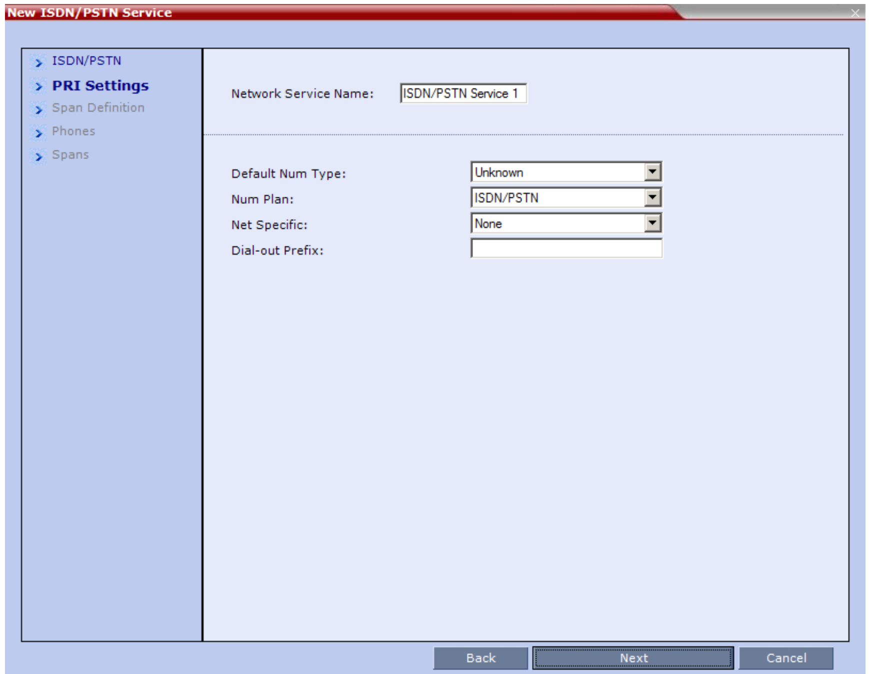
3 Define the following parameters:

Table 16-24 *ISDN Service Settings*

Field	Description
Network Service Name	Specify the service provider's (carrier) name or any other name you choose, using up to 20 characters. The Network Service Name identifies the ISDN/PSTN Service to the system. Default name: ISDN/PSTN Service **Note**: This field is displayed in all ISDN/PSTN Network Properties tabs and can contain character sets that use Unicode encoding.
Span Type	Select the type of spans (ISDN/PSTN) lines, supplied by the service provider, that are connected to the RMX. Each span can be defined as a separate Network Service, or all the spans from the same carrier can be defined as part of the same Network Service. Select either: • **T1** (U.S. – 23 B channels + 1 D channel) • **E1** (Europe – 30 B channels + 1 D channel) Default: T1
Service Type	PRI is the only supported service type. It is automatically selected.

4 Click **Next**.

The *PRI Settings* dialog box is displayed:



5 Define the following parameters:

Table 16-25 *PRI Settings*

Field	Description
Default Num Type	Select the Default Num Type from the list. The Num Type defines how the system handles the dialing digits. For example, if you type eight dialing digits, the Num Type defines whether this number is national or international. If the PRI lines are connected to the RMX via a network switch, the selection of the Num Type is used to route the call to a specific PRI line. If you want the network to interpret the dialing digits for routing the call, select **Unknown**. Default: Unknown **Note:** For E1 spans, this parameter is set by the system.
Num Plan	Select the type of signaling (Number Plan) from the list according to information given by the service provider. Default: ISDN **Note:** For E1 spans, this parameter is set by the system.
Net Specific	Select the appropriate service program if one is used by your service provider (carrier). Some service providers may have several service programs that can be used. Default: None

***Table 16-25** PRI Settings (Continued)*

Field	Description
Dial-out Prefix	Enter the prefix that the PBX requires to dial out. Leave this field blank if a dial-out prefix is not required. The field can contain be empty (blank) or a numeric value between **0** and **9999**. Default: Blank

6 Click **Next**.

The *Span Definition* dialog box is displayed:

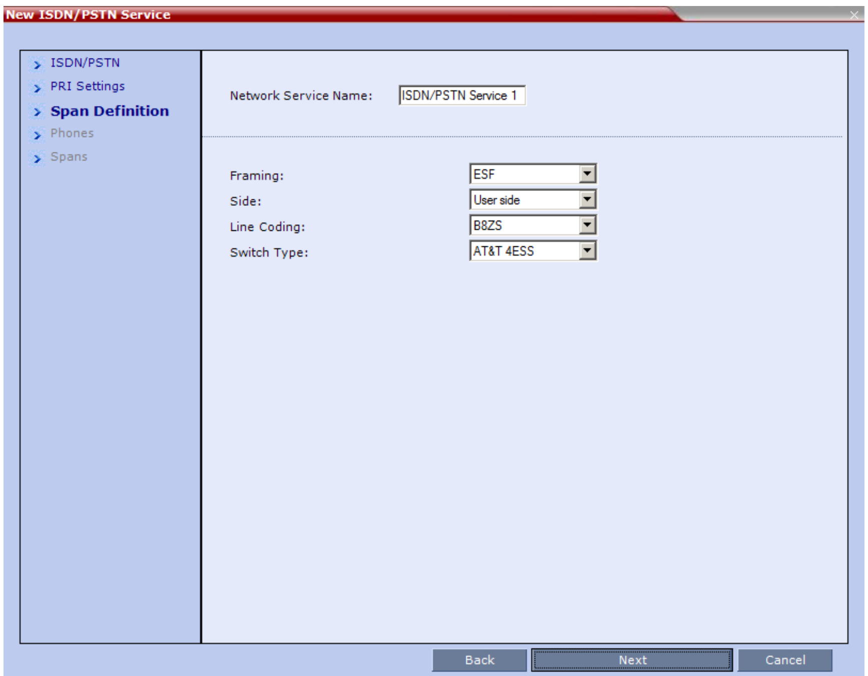


***Table 16-26** Span Definition*

Field	Description
Framing	Select the Framing format used by the carrier for the network interface from the list. • For T1 spans, default is SFSF. • For E1 spans, default is FEBE.
Side	Select one of the following options: • User side (default) • Network side • Symmetric side **Note:** If the PBX is configured on the network side, then the RMX unit must be configured as the user side, and vice versa, or both must be configured symmetrically.

Table 16-26 Span Definition (Continued)

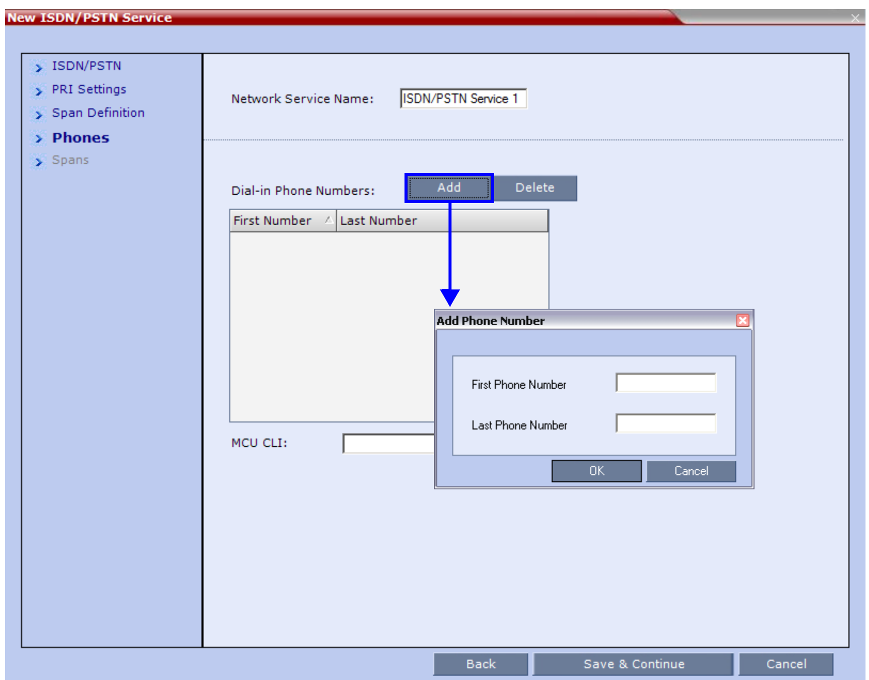
Field	Description
Line Coding	Select the PRI line coding method from the list. • For T1 spans, default is B8ZS. • For E1 spans, default is HDB3.
Switch Type	Select the brand and revision level of switch equipment installed in the service provider's central office. • For T1 spans, default is AT&T 4ESS. • For E1 spans, default is EURO ISDN. **Note:** For T1 configurations in Taiwan, Framing must be set to *ESF* and Line Coding to *B8ZS*.

7 Click **Next**.

The *Phones* dialog is displayed.

8 To define dial-in number ranges click the **Add** button.

9 The *Add Phone Number* dialog box opens.



10 Define the following parameters:

Table 16-27 Phones Settings

Field	Description
First Number	The first number in the phone number range.
Last Number	The last number in the phone number range.

- A range must include at least two dial-in numbers.
- A range cannot exceed 1000 numbers.

11 Click **OK**.

The new range is added to the *Dial-in Phone Numbers* table.

12 **Optional**. Repeat steps **8** to **10** to define additional dial-in ranges.

13 Enter the *MCU CLI* (Calling Line Identification).

In a dial-in connections, the *MCU CLI* indicates the MCU's number dialed by the participant. In a dial-out connection, indicates the MCU (CLI) number as seen by the participant

14 Click **Save & Continue**.

After clicking **Save & Continue**, you cannot use the **Back** button to return to previous configuration dialog boxes.

The ISDN/PSTN Network Service is created and confirmed.

15 Click **OK** to continue the configuration.

The *Spans* dialog box opens displaying the following read-only fields:

— ***ID*** – The connector on the ISDN/PSTN card (PRI1 - PRI12).

— ***Slot*** – The media card that the ISDN/PSTN card is connected to (1 or 2)

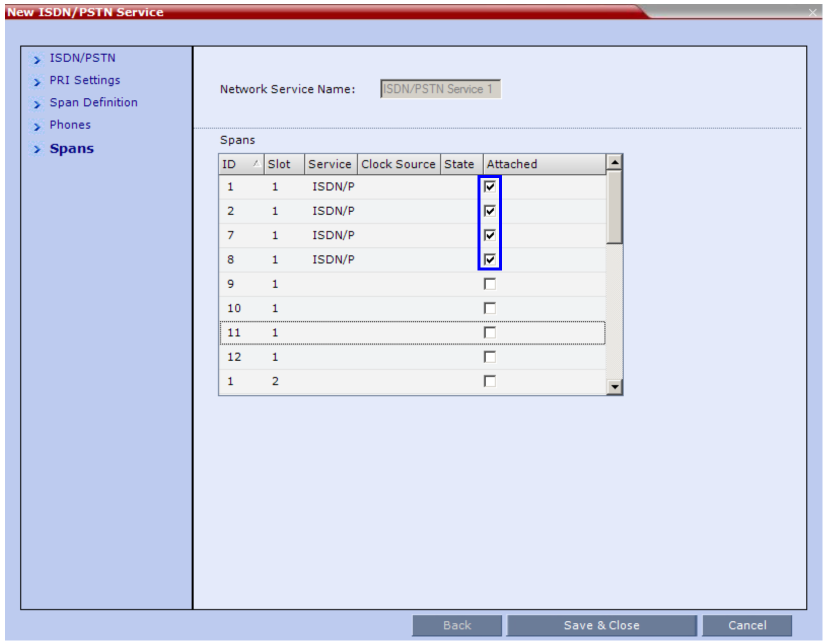
— ***Service*** – The Network Service to which the span is assigned, or blank if the span is not assigned to a Network Service

— ***Clock Source*** – Indicates whether the span acts as a clock source, and if it does, whether it acts as a Primary or Backup clock source. The first span to synchronize becomes the primary clock source.

— ***State*** – The type of alarm: No alarm, yellow alarm or red alarm.

16 Attach spans to existing Network Services, by marking the appropriate check boxes in the *Attached* field.

Each ISDN/PSTN card can support 7 E1 or 9 T1 PRI lines.



17 Click **Save & Close**.

Modifying an ISDN/PSTN Network Service

To Modify an ISDN/PSTN Network Service:

1 In the *RMX Management pane*, click the **ISDN/PSTN Network Services** ( ) icon.

2 In the *ISDN/PSTN Network Services* list, double-click the **ISDN** or right-click the **ISDN** entry and select **Properties**.

The *ISDN Properties* dialog boxes are displayed. They are similar to the *Fast Configuration Wizard's* dialog boxes. For more information see "*To Add an ISDN/PSTN Network Service:*" on page **16-41**.

The following *ISDN Properties* can be modified:

— PRI Settings
- *Net Specific*
- *Dial-out Prefix*

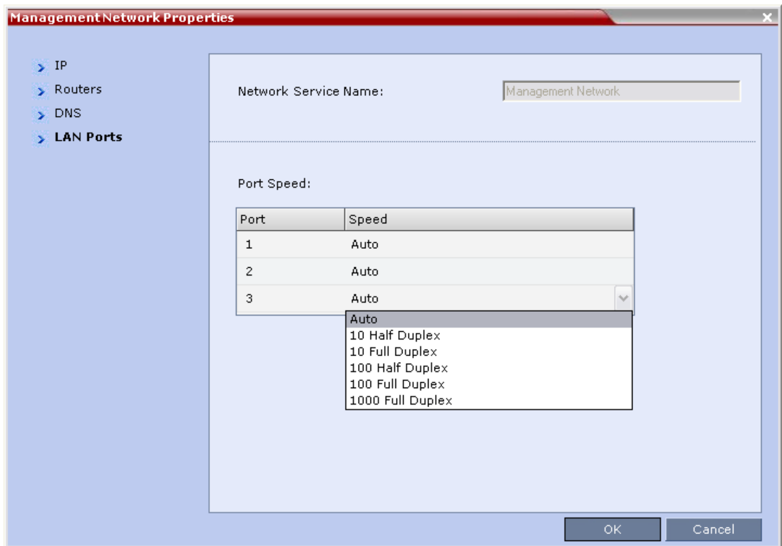
— **Span Definition**
- *Framing*
- *Side*
- *Line Coding*
- *Switch Type*

— **Phones**
- *Dial-in Phone Numbers*
- *MCU CLI*

— Spans
  - *Attached*

All other *ISDN Properties* can only be modified only by deleting the ISDN/PSTN network service and creating a new PSTN service using the *Fast Configuration Wizard*. For more information, see "*To Add an ISDN/PSTN Network Service:*" on page 16-41.

3 Click the **LAN Ports** tab



4 Modify the following fields:

Table 16-28 Default Management Network Service – LAN Ports

Field	Description	
Port Speed	The RMX has 3 LAN ports. The administrator can set the speed and transmit/receive mode manually for **LAN 2** Port only.	
	Port	The LAN port number: 1, 2 or 3. **Note:** Do not change the automatic setting of Port 1 and Port 3. Any change to Port 1 speed will not be applied.
	Speed	Select the speed and transmit/receive mode for each port. Default: Auto – Negotiation of speed and transmit/receive mode starts at 1000 Mbits/second Full Duplex, proceeding downward to 10 Mbits/second Half Duplex. **Note:** To maximize conferencing performance, especially in high bit rate call environments, a 1Gb connection is recommended.

Network Security

System security can be enhanced by separating the *Media*, *Signaling* and *Management Networks*.

RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 4000

On the RealPresence Collaboration Server (RMX) 1500 and RealPresence Collaboration Server (RMX) 4000, Media, Signaling and *Management Networks* are physically separated to provide enhanced security. The *IP Network Service* and the *Default Management Network* have been logically and physically separated from each other. In the *IP Network Service* each IP address is assigned a physical port and media (RTP) inputs are routed directly to an *MPM+* or *MPMx* card. This provides for a more secure network with greater bandwidth as each media card has its own dedicated port. All signaling communications are processed on a single stack of the processor in the RMX.

RealPresence Collaboration Server (RMX) 2000

On the RealPresence Collaboration Server (RMX) 2000 a *RTM LAN* or *RTM ISDN* card is required to enable the separation between the networks. By defining *Multiple Network Services*, a separate network can be defined for each media card installed in the system.

Multiple Network Services

Media, signaling and management networks can be physically separated on the RMX system to provide enhanced security. This addresses the requirement in an organization that different groups of participants be supported on different networks. For example, some participants may be internal to the organization while others are external.

Up to eight media and signaling networks can be defined for the RealPresence Collaboration Server (RMX) 4000, or four for the RealPresence Collaboration Server (RMX) 2000 and two for the RealPresence Collaboration Server (RMX) 1500. Multiple *IP Network Services* can be defined, or up to two (RealPresence Collaboration Server (RMX) 1500)for each media and signaling network connected to the RMX. The networks can be connected to one or several Media cards in the RMX unit.

The *Management Network* is logically and physically separated from the media and signaling networks. There can be one *Management Network* defined per RMX system.

Each conference on the RMX can host participants from the different IP Network networks simultaneously.

The following figure shows the network topology with three different media and signaling networks and one Management network connected to the RealPresence Collaboration Server (RMX) 4000.

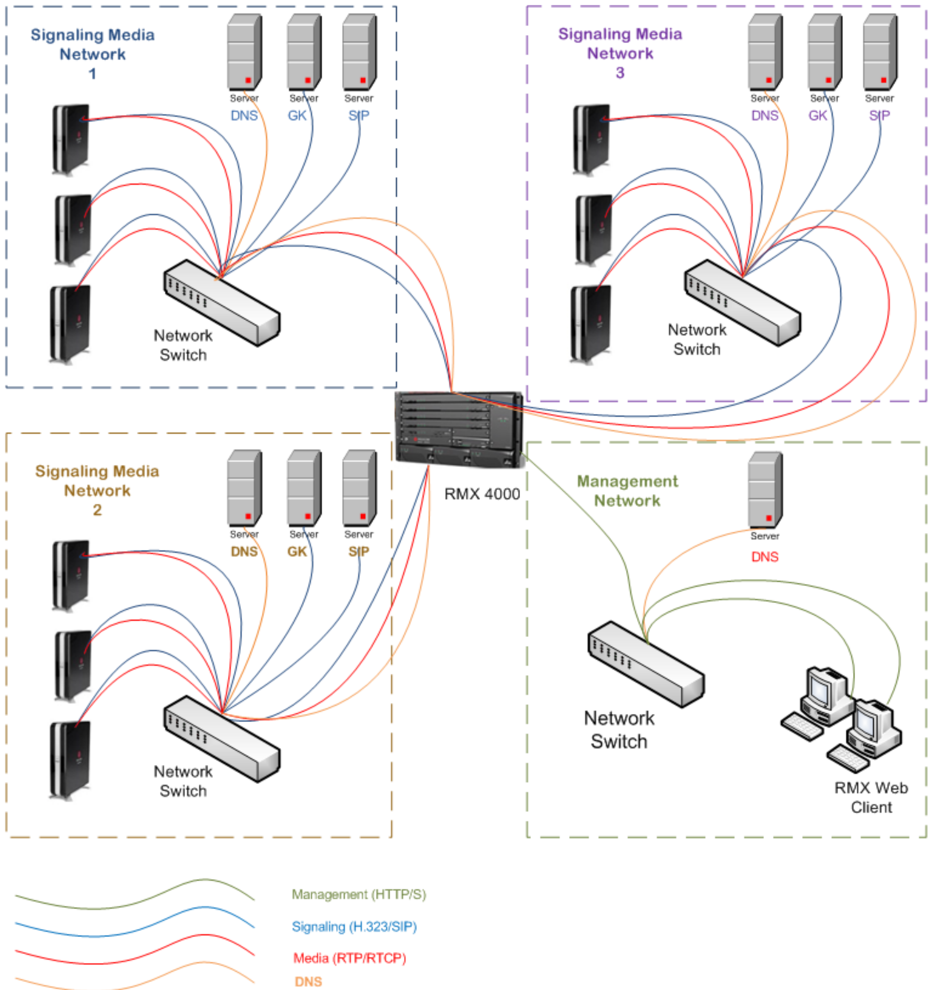


Figure 16-5 RealPresence Collaboration Server (RMX) 4000 - Multiple Network Topology Sample

Guidelines

- Multiple Services system mode is a purchasable option and it is enabled in the MCU license.
- Multiple Services system mode is enabled when the system configuration flag **MULTIPLE_SERVICES** is added and set to **YES**.

The *MULTIPLE_SERVICE System Flag* cannot be set to **YES** when *IPv6 Addressing* is enabled.

- This option is supported with MPM+ and MPMx media cards.
- Multiple Network Services are supported in MCUs with at least 1024MB memory only. MCU units with memory of 512MB support only one IP Network Service.
- Multiple Network Services are not supported with Microsoft ICE Environments in versions prior to *Version 7.8*.
- Only IPv4 is supported for the definition of Multiple Network Services.

- On the RealPresence Collaboration Server (RMX) 1500, up to two Network Services, one per LAN port, can be associated with each Media card.
- On the RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000, RTM ISDN or RTM LAN can be used for Multiple Services configuration. However, if RTM ISDN is installed and used for Multiple Services configuration, only one Network Service can be associated with the media card to which the RTM ISDN card is attached.
- On the RealPresence Collaboration Server (RMX) 1500, when Multiple Network Services option is enabled, the two networks must differ in their subnet masks.
- On the RealPresence Collaboration Server (RMX) 1500, LAN redundancy cannot be enabled in parallel to Multiple Networks and the **LAN_REDUNDANCY** flag must be set to **NO** when the Multiple Networks option is enabled.
- An IP Network Service can be associated with one or several media cards.
- If more than one card is associated with the same Network Service, the system routes the calls to the appropriate card according to resource availability.
- Participants on different networks can connect to the same conference with full audio, video and content capabilities.
- Traffic on one network does not influence or affect the traffic on other networks connected to the same MCU, unless they are connected to the same media card. If one network fails, it will not affect the traffic in the other connected networks, unless they are connected to the same media card and the card fails.
- Maximum number of services that can be defined per RMX platform:

Table 16-29 *Maximum Number of Network Services per RMX System*

RMX	Total Media Cards	Network Services (Up to 2 per Media Card)	Management Services	Network Services that Include ICE (1 / Media Card)
1500	1	Up to 2	1	1
2000	2	Up to 2 (combination of RTM ISDN and/or RTM LAN) or Up to 4 (using 2 RTM LAN cards, less when using up to 2 RTM ISDN cards)	1	2
4000	4	Up to 4 (Up to 2 RTM ISDN cards and the remaining RTM LAN cards) Up to 8 (using 4 RTM LAN, less when using up to 2 RTM ISDN cards)	1	4

- Prior to *Version 7.8*, only one *DNS* server could be defined for the entire configuration From *Version 7.8* onwards, a *DNS* server can be specified for each *IP Network Service* and for the RMX *Management Network Service*.
  — In the Network Services that do not include the DNS, use the IP addresses of the various devices to define them in the Network Services.

- Participants are associated with a Network Service and use it resources as follows:
  - Dial-in participants - according to the network used to place the call and connect to the RMX.
  - Dial-out participant - according to the Network Service selected during the participant properties definition or during conference definition, according to the Network Service selected as default.

Resource Allocation and Capacity

The *Video/Voice Port Configuration* and the *Resolution Configuration* settings are configured per MCU and affect the resource capacity of the MCU. They are reflected in the port gauges displayed on the RMX management application's main screen. In *Multiple Networks* mode, the overall resources as configured in the *Video/Voice Port Configuration* are divided between the Network Services. However, the port gauges do not reflect the resource availability per Network Service.

Fixed and Flexible Resource Allocation Mode

On the RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000 resources are divided between services according to the number of media cards associated with each service and the card assembly type (for example, MPMx-s vs. MPMx-D). If two identical media cards are installed in the system and each card is assigned to a different Network Service, the resources are split between the services.

If two cards are installed but each card is of different assembly type, the resources are allocated according to the card capacity ratio. For example, in a system with one MPMx-S and one MPMx-D, the capacity ratio is 1 to 2, therefore a third of the resources will be assigned to the network service associated with MPMx-S and two thirds will be assigned to the Network Service associated with MPMx-D.

On the RealPresence Collaboration Server (RMX) 1500 and the RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000 with two *Network Services* associated with one media card, the resources of the two Network Services associated with one media card are not split between the network services. In such a case, resources are used per their availability by both Network Services equally.

On the RealPresence Collaboration Server (RMX) 2000, if RTM ISDN is installed and used for Multiple Services configuration, only one Network Service can be defined per media card.

In *Fixed Resource Allocation Mode* if the resources cannot be divided into whole numbers, they will be rounded up to the nearest whole number, assigning that resource to the *Network Service* with the higher capacity (i.e. more media cards or media cards with higher capacity due to a different card assembly).

First Time Installation and Configuration

First Time Installation and Configuration of the Polycom RealPresence Collaboration Server (RMX) 1500/2000/4000 consists of the following procedures:

1 **Preparations**
   - Gather Network Equipment and Address Information - get the information needed for integrating the RMX into the local network for each of the networks that will be connected to the RMX unit. For a list of required address, see the *RealPresence*

Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide Getting Started Guide, "Gather Network Equipment and Address Information" on page **2-1**.

2 **Hardware Installation and Setup**

— Mount the RMX in a rack. For more details see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide Getting Started Guide, "Hardware Installation and Setup"* on page **2-8**.

— Connect the necessary cables. For details, see *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide Getting Started Guide, "Hardware Installation and Setup"* on page **2-8**.

3 **First Entry Power-up and Configuration**

— Power up the RMX. For more details see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide Getting Started Guide, "Procedure 1: First-time Power-up"* on page **2-25**.

— Register the RMX. For more details see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide Getting Started Guide, "Procedure 2: Product Registration"* on page **2-26**.

— Connect to the RMX. For more details see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide Getting Started Guide, "Procedure 3: Connection to MCU"* on page **2-26**.

— Configure the *Default IP Network Service* using the information for one of the networks connected a media card installed in the system. For more details see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide Getting Started Guide, "Procedure 4: Modifying the Default IP Service and ISDN/PSTN Network Service Settings"* on page **2-28**.

— **Optional.** Configure the *ISDN/PSTN Network Service*. For more details see the *.RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide Getting Started Guide, "ISDN/PSTN Services"* on page **2-3**.

4 Modify the required System Flag to enable Multiple Services and reset the MCU.

5 Add the required IP Network Services to accommodate the networks connected to the RMX.

6 Select a Network Service to act as default for dial out and gateway calls for which the Network Service was not selected.

7 Place several calls and run conferences to ensure that the system is configured correctly."*Gather Network Equipment and Address Information - IP Network Services Required Information"* on page **16-40**.

Upgrading to Multiple Services

1 Gather Network Equipment and Address Information for each of the networks that will be connected to the RMX unit. For a list of required address, see *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "Gather Network Equipment and Address Information"* on page **2-2**.

2 Upgrade to the new version and install the activation key that contains the Multiple Services license as described in the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Release Notes*.

3 Place several calls and run conferences to ensure that the system upgrade was completed successfully.

4 Modify the required System Flag to enable Multiple Services, DO NOT reset the MCU yet.

5 Connect the additional network cables to the RMX and change existing connections to match the required configuration as described in the "*RealPresence Collaboration Server (RMX) Hardware Installation"* on page **16-55**.

At this point, the Management Network can be modified to match the required local network settings.

> If the RealPresence Collaboration Server (RMX) 2000 you are upgrading does not include RTM ISDN or RTM LAN cards, you must install at least one RTM LAN card to enable the definition of multiple Network Services. If no RTM ISDN or RTM LAN cards are installed, the RealPresence Collaboration Server (RMX) 2000 works in a single Network Service mode and an alarm is issued by the system. For more details about the installation of RTM LAN cards, see the *RealPresence Collaboration Server (RMX) 2000 Hardware Guide*.

6 Reset the MCU.

7 Connect to the MCU and Add the required IP Network Services to accommodate the networks connected to the RMX unit.

8 Select a Network Service to act as default for dial out and gateway calls for which the Network Service was not selected.

9 Place several calls and run conferences to ensure that the system is configured correctly.

Gather Network Equipment and Address Information - IP Network Services Required Information

It is important that before connecting multiple networks and implementing Multiple Services in the RMX, that you obtain the information needed to complete the **IP Network Service** configuration for each connected network from your network administrator.

Table 16-30 *Network Equipment and Address Information per IP Network Service*

Parameter	Local Network Settings	Note
Signaling Host IP address		
Media Board IP address (MPM 1)		
Media Board IP address (MPM 2) ***RealPresence Collaboration Server (RMX) 2000/ RealPresence Collaboration Server (RMX) 4000 only***		If more than one media card is associated with this Network Service
Media Board IP address (MPM 3) ***RealPresence Collaboration Server (RMX) 4000 only***		If more than one media card is associated with this Network Service

Table 16-30 Network Equipment and Address Information per IP Network Service (Continued)

Parameter	Local Network Settings	Note
Media Board IP address (MPM 4) ***RealPresence Collaboration Server (RMX) 4000 only***		If more than one media card is associated with this Network Service
Gatekeeper IP address (optional)		
DNS IP address (optional)		Only one DNS can be defined for the entire Network topology
SIP Server IP address (optional)		

RealPresence Collaboration Server (RMX) Hardware Installation

When connecting the LAN cables of the various networks to the RMX it is recommended to use a color system to differentiate between the networks, for example, using colored cables.

RealPresence Collaboration Server (RMX) 4000 Multiple Services Configuration

Connecting the cables to the RTM IP 4000:

The following cables are connected to the RTM IP on the rear panel of the RealPresence Collaboration Server (RMX) 4000:

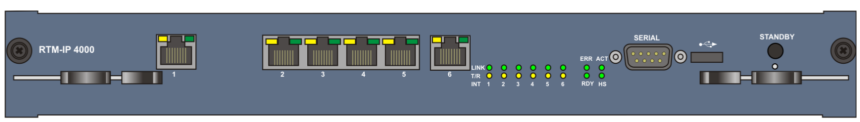


Table 16-31 LAN Connections to the RTM IP

RTM IP Port	Description
LAN 1	Modem
LAN 2	Management
LAN 3	–
LAN 4	–
LAN 5	–
LAN 6	Shelf Management

Connecting the cables to the RTM LAN:

Table 16-32 LAN Connections to the RTM LAN

RTM LAN Port	Description
LAN 1	Signaling and Media - additional (second) Network Service
LAN 2	Signaling and Media - existing (first) Network Service

Figure 16-6 shows the cables connected to the RealPresence Collaboration Server (RMX) 4000 rear panel, when one RTM ISDN and three RTM LAN cards are installed providing IP and ISDN connectivity. The RTM ISDN card can be used for both ISDN and IP calls and only one IP network Service is associated with each RTM LAN card.

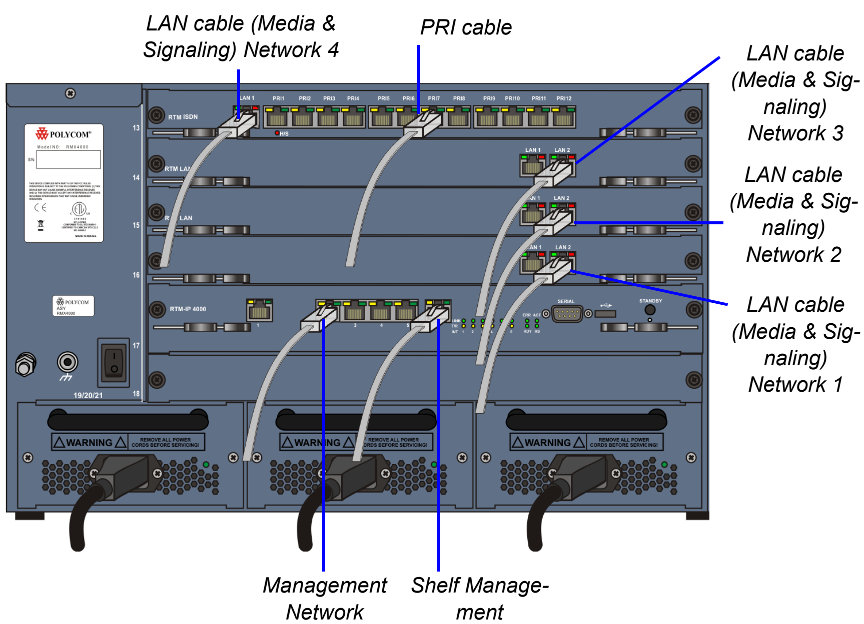


Figure 16-6RealPresence Collaboration Server (RMX) 4000 Rear Panel with LAN and PRI cables

In this case, up to four different IP Network Services can be defined - one for each RTM LAN/RTM ISDN cards installed in the system.

If two LAN ports per each installed RTM LAN card are used, up to three additional Network Services can be defined, bringing it to a total of up to 7 IP Network Services.

Several cards can be assigned to the same IP Network Service. The definition of the network services attached to the RMX unit and which cards are assigned to each network service is defined in the IP Network Service.

RealPresence Collaboration Server (RMX) 2000 Multiple Services Configuration

Connecting the cables to the RTM IP:

The following cables are connected to the RTM IP on the rear panel of the RealPresence Collaboration Server (RMX) 2000:

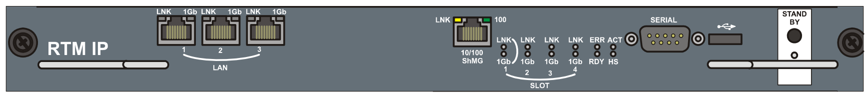


Table 16-33 LAN Connections to the RTM IP

RTM IP Port	Description
LAN 1	–
LAN 2	Management
LAN 3	Modem

Connecting the cables to the RTM LAN:

If RTM LAN or RTM ISDN cards are not installed on the RMX, they must be installed before connecting the additional network cables for media and signaling.

Table 16-34 LAN Connections to the RTM LAN

RTM IP Port	Description
LAN 1	Signaling and Media - second Network Service (optional)
LAN 2	Signaling and Media - first Network Service (optional)

If one LAN port per RTM ISDN/ RTM LAN card is used, up to two different IP Network Services can be defined - one for each installed RTM LAN/RTM ISDN cards.

If two LAN ports per each installed RTM LAN card are used, up to four Network Services can be defined.

Figure 16-7 shows the cables connected to the RealPresence Collaboration Server (RMX) 2000 rear panel, when two RTM LAN cards are installed providing IP connectivity. In this case, only one IP network Service can be associated with each RTM LAN card.

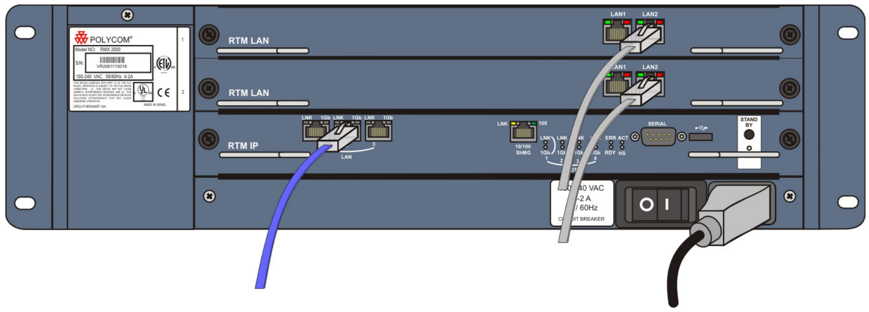


***Figure 16-7** RealPresence Collaboration Server (RMX) 2000 Rear Panel with RTM LAN Cables*

RealPresence Collaboration Server (RMX) 1500 Multiple Services Configuration

Connecting the cables to the RTM IP 1500:

The following cables are connected to the RTM IP on the rear panel of the RealPresence Collaboration Server (RMX) 1500:

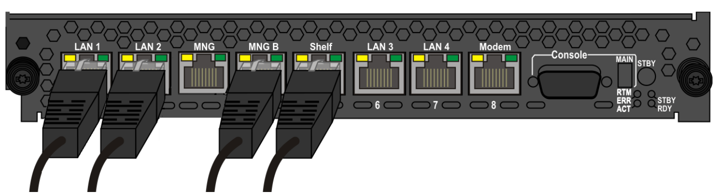


***Table 16-35** LAN Connections to the RTM IP*

RTM IP Port	Description
LAN 1	Media and signaling - additional (second) Network Service
LAN 2	Media and signaling - existing (first) Network Service
MNG	–
MNG B	Management
Shelf	Shelf Management
LAN 3	–
LAN 4	–
Modem	Modem

RMX Configuration

Once the network cables are connected to the RMX, you can modify the default IP Network Service and add additional Network Services.

System Flags and License Settings

The **MULTIPLE_SERVICES** System Flag determines whether the Multiple Services option will be activated once the appropriate license is installed. Possible Values: **YES / NO**
Default: **NO**

This flag must be manually added to the system configuration and set to YES to enable this option. For more information see "*Manually Adding and Deleting System Flags"* on page **22-18**.

> If the MULTIPLE_SERVICES System Flag is set to YES and no RTM ISDN or RTM LAN card is installed in the RealPresence Collaboration Server (RMX) 2000, an Active Alarm is displayed.

> If the values or either of the MULTIPLE_SERVICES or V35_ULTRA_SECURED_SUPPORT *System Flags* are changed from YES to NO, the defined *IP Network Services* are not displayed in the *IP Network Services* list pane: they are, however, saved in the system.
> If either of the flag values are changed back to YES, the saved defined *IP Network Services* will be displayed.

IP Network Service Definition

Use this procedure to define Network Services in addition to the Network Service already defined during first entry installation and configuration. Each of the defined Network Service can be associated with one or more media cards installed in the system (depending on the system type).

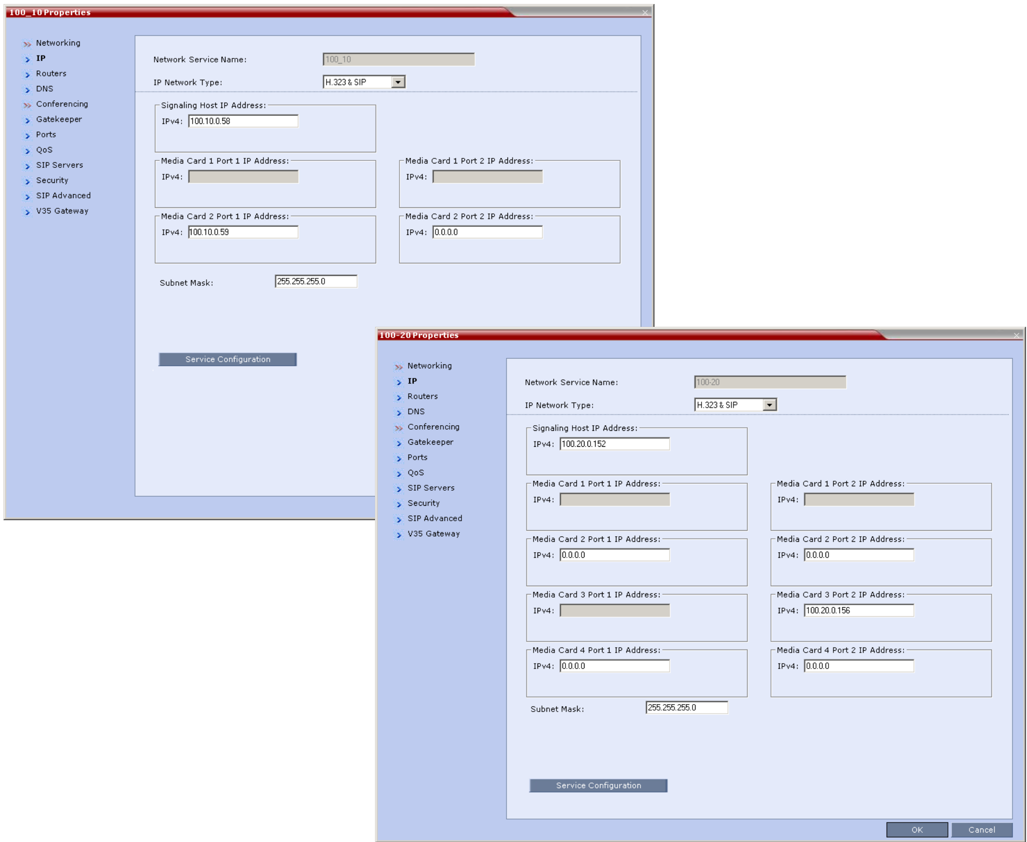
Once a media card is associated with a Network Service it **cannot be** associated with another network service.

To add new/additional Network Services:

1 In the *Device Management* pane, click **IP Network Services** ( ).

2 In the *Network Services* list toolbar, click the **Add Network Service** button.

The *New IP Service - Networking IP* dialog box opens.



3 Define the following fields:

Table 16-36 *IP Network Service - IP Parameters*

Field	Description
Network Service Name	Enter the IP Network Service name. **Note:** This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.
IP Network Type	Select the IP Network environment. You can select: • **H.323:** For an H.323-only Network Service. • **SIP:** For a SIP-only Network Service. • **H.323 & SIP:** For an integrated IP Service. Both H.323 and SIP participants can connect to the RMX using this service. **Note:** This field is displayed in all Default IP Service tabs.
Signaling Host IP Address	Enter the address to be used by IP endpoints when dialing into the RMX using this Network Service. Dial out calls of participants to whom this network service will be assigned are initiated from this address. This address is used to register the RMX with a Gatekeeper or a SIP Proxy server residing on this network.

Table 16-36 *IP Network Service - IP Parameters*

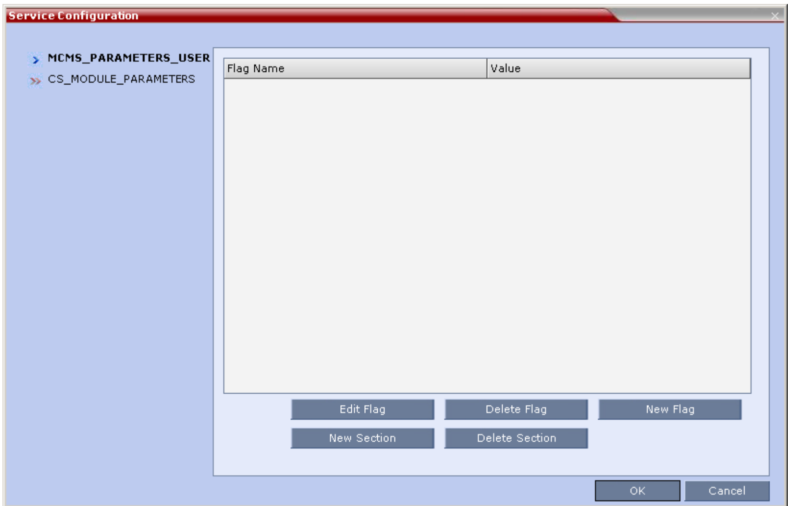
Field	Description
Media Card 1 Port 1 IP Address	If only one network is connected to this media card, it is enough to assign one media card to this Network Service. In such a case, enter one IP address for the media card according to the LAN Port used for the connection. If each of the LAN ports on one media card is used with two different networks, each port is assigned to its own Network Service. In such a case, enter the IP address of the port to be assigned to this Network Service. A LAN port that is already assigned to a different Network Service, displays the IP Address of the assigned port and it cannot be assigned to this Network Service (it is disabled).
Media Card 1Port 2 IP Address 2	
Media Card 2 Port 1 IP Address ***(RealPresence Collaboration Server (RMX) 2000/ RealPresence Collaboration Server (RMX) 4000)***	If only one network is connected to this media card, it is enough to assign one media card to this Network Service. In such a case, enter one IP address for the media card according to the LAN Port used for the connection, as provided by the network administrator. If each of the LAN ports on one media card is used with two different networks, each port is assigned to its own Network Service. In such a case, enter the IP address of the port to be assigned to this Network Service. **Notes:** • LAN Ports/Media cards that are already associated with another Network Service cannot be associated with this Network Service. • You can define a Network Service without assigning media cards to it. • To change the assignment of a card from one service to another, the card must first be removed from the service to which it is assigned prior to its assignment to another service. **RealPresence Collaboration Server (RMX) 2000:** If one card was already assigned to another service, only one additional card can be assigned to this service. **RealPresence Collaboration Server (RMX) 4000:** Depending on the number of media cards installed in the system, you can assign up to 4 media cards to this network service provided that they are not assigned to any other Network Service.
Media Card 2 Port 2 IP Address ***(RealPresence Collaboration Server (RMX) 2000/ RealPresence Collaboration Server (RMX) 4000)***	
Media Card 3 Port 1 IP Address ***(RealPresence Collaboration Server (RMX) 4000)***	
Media Card 3 Port 2 IP Address ***(RealPresence Collaboration Server (RMX) 4000)***	
Media Card 4 Port 1 IP Address ***(RealPresence Collaboration Server (RMX) 4000)***	
Media Card 4 Port 2 IP Address ***(RealPresence Collaboration Server (RMX) 4000)***	

Table 16-36 *IP Network Service - IP Parameters*

Field	Description
Subnet Mask	Enter the subnet mask of the RMX in that network service. Default value: 255.255.255.0.

4 **Optional.** Some system flags can be defined per Network Service, depending on the network environment.
To modify these flags, click the **Service Configuration** button.

The *Service Configuration* dialog box opens.



All the flags must be manually added to this dialog box. For a detailed description of the flags and how to add them, see "*Manually Adding and Deleting System Flags"* on page 22-18.

> Flags defined per Network Service override their general definition in the System Configuration.

The following flags can be defined per service:

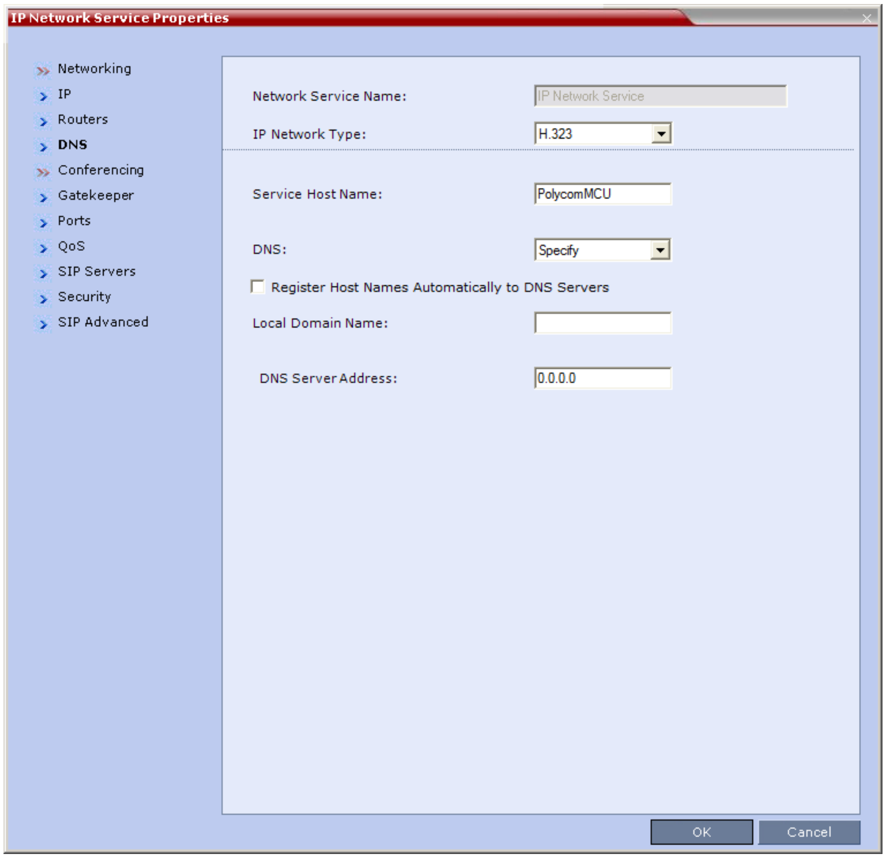
— ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF
— ENABLE_H239
— SIP_ENABLE_FECC
— ENABLE_CLOSED_CAPTION
— ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF
— NUMERIC_CONF_ID_LEN
— NUMERIC_CONF_ID_MIN_LEN
— NUMERIC_CONF_ID_MAX_LEN
— ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD
— MAX_CP_RESOLUTION
— QOS_IP_AUDIO
— QOS_IP_VIDEO
— QOS_IP_SIGNALING
— ENABLE_CISCO_GK

- SIP_FREE_VIDEO_RESOURCES
- FORCE_CIF_PORT_ALLOCATION
- MS_ENVIRONMENT
- SIP_FAST_UPDATE_INTERVAL_ENV
- SIP_FAST_UPDATE_INTERVAL_EP
- H263_ANNEX_T
- H239_FORCE_CAPABILITIES
- MIX_LINK_ENVIRONMENT
- IP_LINK_ENVIRONMENT
- FORCE_STATIC_MB_ENCODING
- FORCE_RESOLUTION
- SEND_WIDE_RES_TO_IP
- DISABLE_WIDE_RES_TO_SIP_DIAL_OUT
- SEND_SIP_BUSY_UPONRESOURCE_THRESHOLD

5 Click the **Routers** tab.

6 Define the routers used in this network and that are other than the routers defined in the Management Network. The field definitions of the *Routers* tab are the same as for the *Default Management Network*. For more information see "*Click the Routers tab."* on page 16-13.

7 Click the **DNS** tab.



8 Modify the following fields:

Table 16-37 *Default Management Network Service – DNS*

Field	Description
Service Host Name	Enter the host name of this network Service. Each Network Service must have a unique Host Name otherwise an error message is displayed.
DNS	Select: • **Off** – if no DNS server is used in this network. • **Specify** – to enter the IP address of the DNS server used by this network service. **Notes:** • The IP address field is enabled only if **Specify** is selected. • Only one DNS can be define for the entire topology (that is, only one Network Service can include the DNS definition).
Register Host Names Automatically to DNS Servers	Select this option to automatically register this Network Service Signaling Host with the DNS server.
Local Domain Name	Enter the name of the domain for this network service.
DNS Server Address	Enter the static IP address of the DNS server that is part of this network.

9 Click the **Gatekeeper** tab.

10 Define the *Primary* and *Alternate Gatekeepers* and at least one **Alias** for this network Service. The field definitions of the *Gatekeeper* tab are the same as for the *Default IP Network Service*. For more information see "*Click the Gatekeeper tab."* on page **16-14**.

In *Multiple Services* mode, an Alias must be defined for the specified gatekeeper.

11 **Optional.** Click the **Ports** tab.

Settings in the *Ports* tab allow specific ports in the firewall to be allocated to multimedia conference calls. If required, defined the ports to be used multimedia conference calls handled by this Network Service. The field definitions of the *Ports* tab are the same as for the *Default IP Network Service*.

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Click the Ports tab."* on page **16-15**.

12 If required, click the **QoS** tab.

The RMX's implementation of *QoS* is defined per Network Service, not per endpoint.

The routers must support QoS in order for IP packets to get higher priority.

The field definitions of the *QoS* tab are the same as for the *Default IP Network Service*. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*If required, click the QoS tab."* on page **16-17**.

13 Click the **SIP Servers** tab.

14 Define the *Primary* and *Alternate SIP Server* for this network Service.

- Starting with Version 7.1, Registration of conferencing entities with the SIP Servers was moved to the conferencing entities and is defined in the Conference Profile.
- If Microsoft Office Communications or Lync server are part of this network service, a certificate must be created for this network service. If each network connected to the RMX includes Microsoft Office Communications or Lync server, separate certificates must be created and sent to the RMX for each of these networks.
- If the Network Service does not include a DNS, you must use the IP address of the SIP Server instead of its name.

The field definitions of the *SIP Servers* tab are the same as for the *Default IP Network Service*. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Click the SIP Servers tab.*" on page **16-19**.

15 Click the **Security** tab.

The field definitions of the *Security* tab are the same as for the *Default IP Network Service*. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Click the Security tab.*" on page **16-21**.

16 **Optional.** To configure the ICE environment, click the **SIP Advanced** tab.

17 Modify the following fields:

Table 16-38 *Default IP Network Service – SIP Advanced*

Field	Description
Server User Name	Enter the *User* name for this service as defined in the *Active Directory*. For example, enter *rmxNet2*. This field is disabled if the *ICE Environment* field is set to *None*.
ICE Environment	Select **MS** (for *Microsoft ICE* implementation) to enable the *ICE* integration. This field is disabled if the RMX is not running in *MPM+ Card Configuration Mode*.

18 Click the **OK** button.
The new Network Service is added to the *IP Network Services* list pane.

Setting a Network Service as Default

The default Network Service is used when no Network Service is selected for the following:

- Dial out participants
- Reserving resources for participants when starting an ongoing conference
- Gateway calls

In addition, the Signaling Host IP address and the MCU Prefix in GK displayed on the *RealPresence Collaboration Server Web Client* main screen are taken from the default H.323 Network Service.

One IP Network Service can be defined as default for H.323 connections and another Network Service as default for SIP connections. If the IP Network Service supports both H.323 and SIP connections, you can set the same Network Service as default for both H.323 and SIP, or for H.323-only or for SIP-only.

To designate an IP Network Service as the default IP Network Service:

1. In the *Device Management* pane, click **IP Network Services** ().
2. In the *Network Services* list pane right-click the IP Network Service to be set as the default, and then click **Set As H.323 Default,** or **Set As SIP Default**.

   The next time you access this menu, a check mark is added next to the network service type to indicate its selection as default.

   To set this IP Network Service for both H.323 and SIP connections, repeat step 2 and select the option you need.

   The following icons are used to indicate the default IP Network Service type:

Table 16-39 Default IP Network Service Icons

Icon	Description
	This Network Service supports both SIP and H.323 connections and is designated as default for both SIP and H.323 connections.
	This Network Service supports both SIP and H.323 connections and is designated as default for H.323 connections.
	This Network Service supports both SIP and H.323 connections and is designated as default for SIP connections.
	This Network Service supports only H.323 connections and is set as default for H.323 connections.
	This Network Service supports only SIP connections and is set as default for SIP connections.

Ethernet Settings

The RealPresence Collaboration Server (RMX) 2000 is set to automatically identify the speed and transmit/receive mode of each LAN ports located on the RTM LAN or RTM ISDN cards that are added to the system. These port settings can be manually configured if the specific switch requires it, via the **Ethernet Settings** as for the RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 4000. For more details, see "*Ethernet Settings"* on page 16-24.

RealPresence Collaboration Server (RMX) 1500: The *Port* numbers displayed in the dialog box do not reflect the physical *Port* numbers as labeled on the RealPresence Collaboration Server (RMX) 1500 MCU.

Signaling Host IP Address and MCU Prefix in GK Indications

The *RealPresence Collaboration Server Web Client* displays the *Signaling Host IP Address* and *MCU Prefix in GK* parameters as defined in the **Default H.323 Network Servic**e.

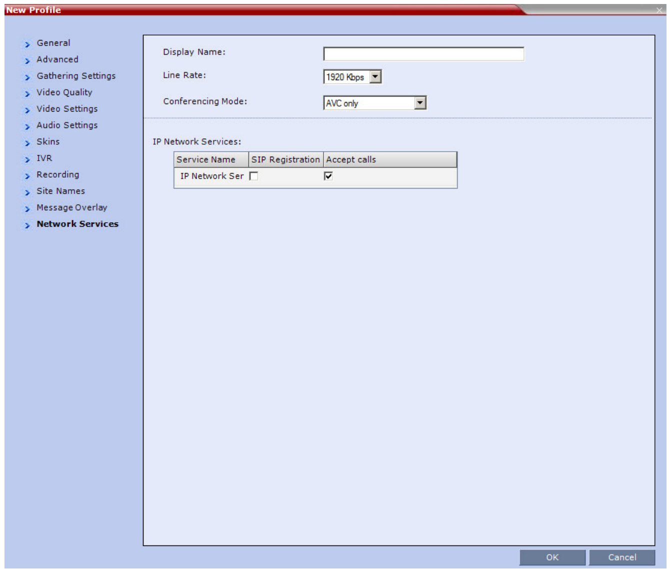
Video/Voice Port Configuration and Resolution Configuration

These configurations are set for the system and are applied to all the Network Services.

Conference Profile

Registration of conferencing entities such as ongoing conferences, Meeting Rooms, Entry Queues, SIP Factories and Gateway Sessions with SIP servers is done per conferencing entity. This allows better control on the number of entities that register with each SIP server by selecting for each of the conferencing entities whether it will register with the SIP server.

The registration is defined in the *Conference Profile - Network Services* tab.



In the *IP Network Services* table, the system lists all the defined Network Services (one or several depending on the system configuration).

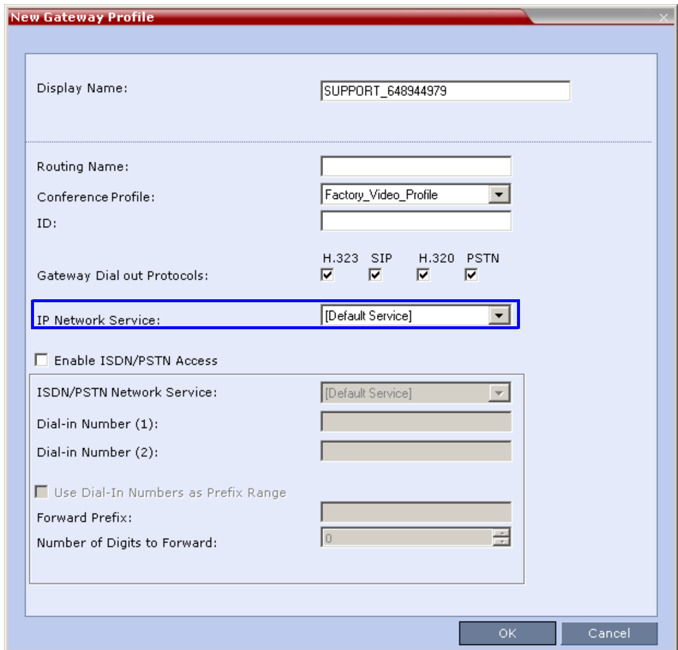
- To register the conferencing entity to which this profile is assigned to a Network Service, in the *Registration* column click the check box of that Network Service.
- You can also prevent dial in participants from connecting to that conferencing entities when connecting via a Network Service.
  In the *Accept Calls* column, clear the check box of the Network Service from which calls cannot connect to the conference.

Gateway Profiles

To enable the RMX to call the destination endpoint/MCU via IP connection, the Network Service for the call must be selected in the Gateway Profile dialog box.

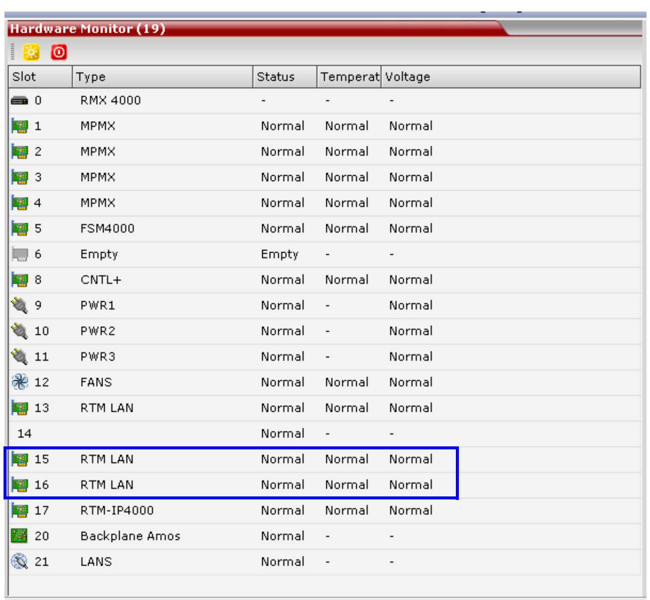
The Network Service set as default is used if no other Network Service is selected.

If the same Network Service is used for H.323 and SIP calls, the *Network Service Environment* must include both **H.323** and **SIP** settings.



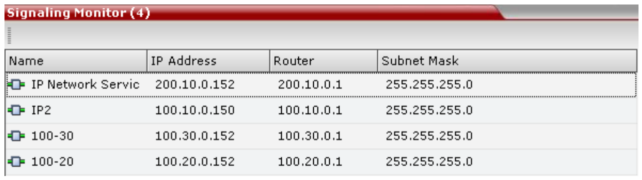
Hardware Monitor

The Hardware Monitor pane includes the status of the LAN ports on the RTM LAN cards.



Signaling Monitor

The Signaling Monitor pane includes the list of the IP Network Services defined in the system (up to two in the RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 2000 and up to four in the RealPresence Collaboration Server (RMX) 4000). Double-clicking a Network Service, displays it properties and status.



Conferencing

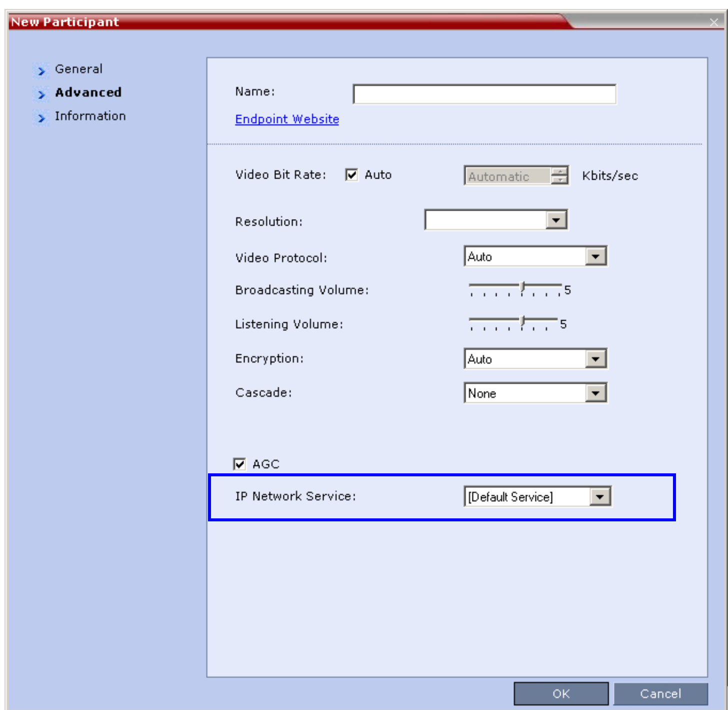
Each conference on the RMX can host participants from the different IP Network networks simultaneously.

Defining Dial Out Participants

When defining dial out participants, you can select the Network Service to place the call according to the network to which the endpoint pertains. If the endpoint is located on a network other than the selected network, the participant will not be able to connect.

If no Network is selected, the system uses the IP Network Service selected for reserving the conference resources, and if none is set for the conference it uses the Network Service set as default.

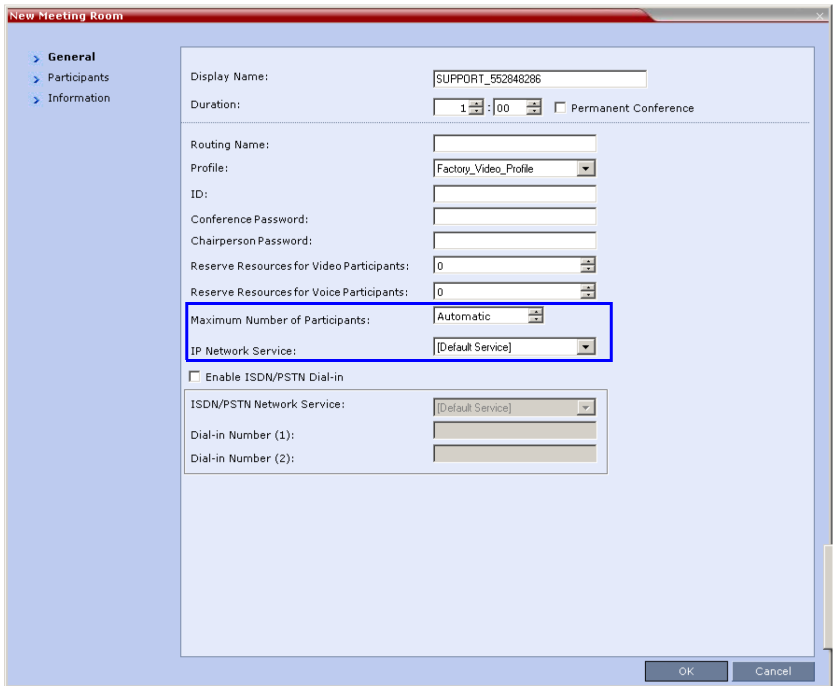
The IP Network Service is selected in the *New Participant - Advanced* dialog box.



Reserving Video Resources for a Conference

When defining a new ongoing conference or a conference reservation, you can select the Network Service that will be used to reserve the required resources. If no Network Service is selected, the default Network Service is used. Therefore, make sure that not all conferences are reserving resources from the same Network Service, otherwise you may run out of resources for that Network Service.

The IP Network Service is selected in the *New Conference/New Meeting Room/New Reservation - General* dialog box.



Monitoring Conferences

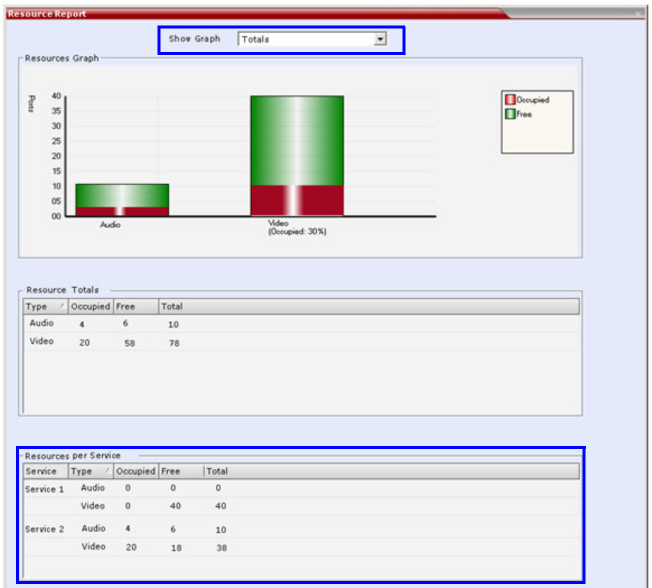
The *Conference Properties - Network Services* dialog box shows for each Network Service with which Network Service’s SIP proxy the conference should be registered and if the dial in call will be connected to the conference.

In the *Participant* pane, a new column - *Service Name* was added, indicating the name of Network Service used for the participant’s connection.

Resource Report

The *Resource Report* displays the resource usage in total and per Network Service in a table format. The Resources per Service table provides the actual information on resource usage and availability per network Service and provides an accurate snapshot of resources usage in the system.

You can select the graph to display: select either **Totals** (default) or the Network Service.



Port Gauge Indications

The port Gauges displays the total resource usage for the RMX and not per Network Service. Therefore, it may not be an accurate representation of the availability of resources for conferencing, as one Network Service may run out of available resources while another Network Service may have all of it resources available. In such a case, the port gauges may show that half of the system resources are available for conferencing, while calls via the Network Service with no available resources will fail to connect.

NAT (Network Address Translation) Traversal

NAT Traversal is a set of techniques enabling participants behind firewalls to connect to conferences, hosted on the RMX, remotely using the internet.

Session Border Controller (SBC)

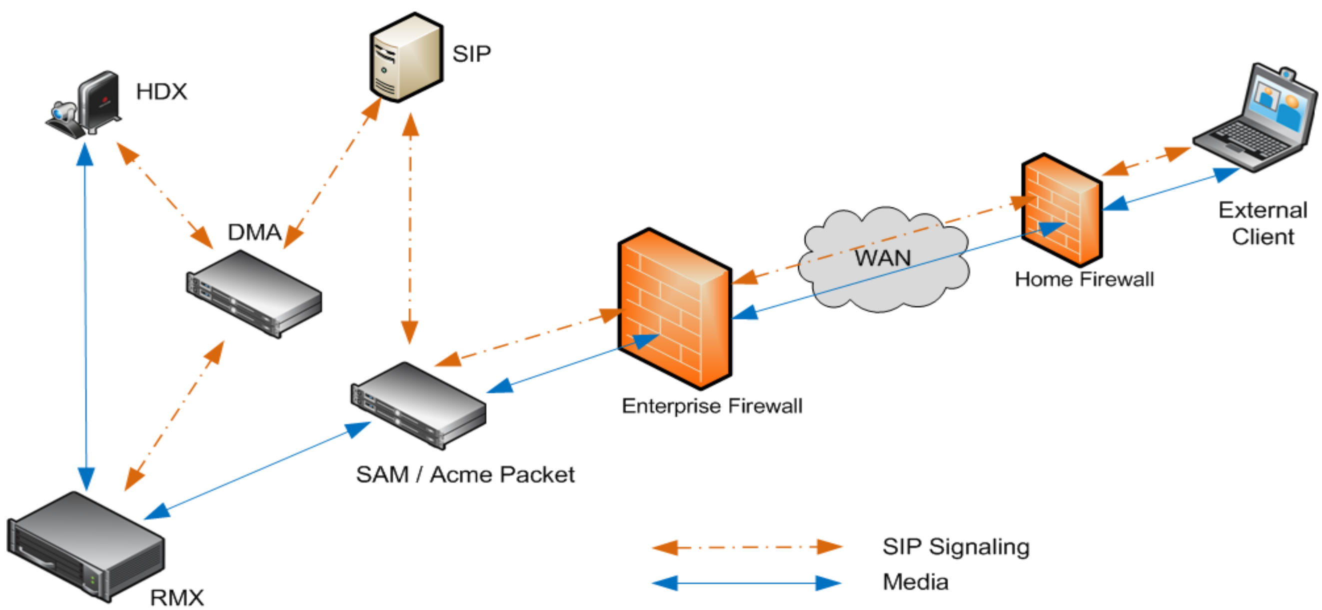
All signaling and media for both SIP and H.323 will be routed through an *SBC*.
The following *SBC* environments are supported:

- *SAM* - a *Polycom SBC*
- *Acme Packet* - a 3rd party *SBC*
- *VBP* - *Polycom Video Border Proxy*

Deployment Architectures

The following *NAT Traversal* topologies are given as examples. Actual deployments will depend on user requirements and available infrastructure:

Remote Connection Using the Internet



The following *Remote Connection* call flow options are supported:

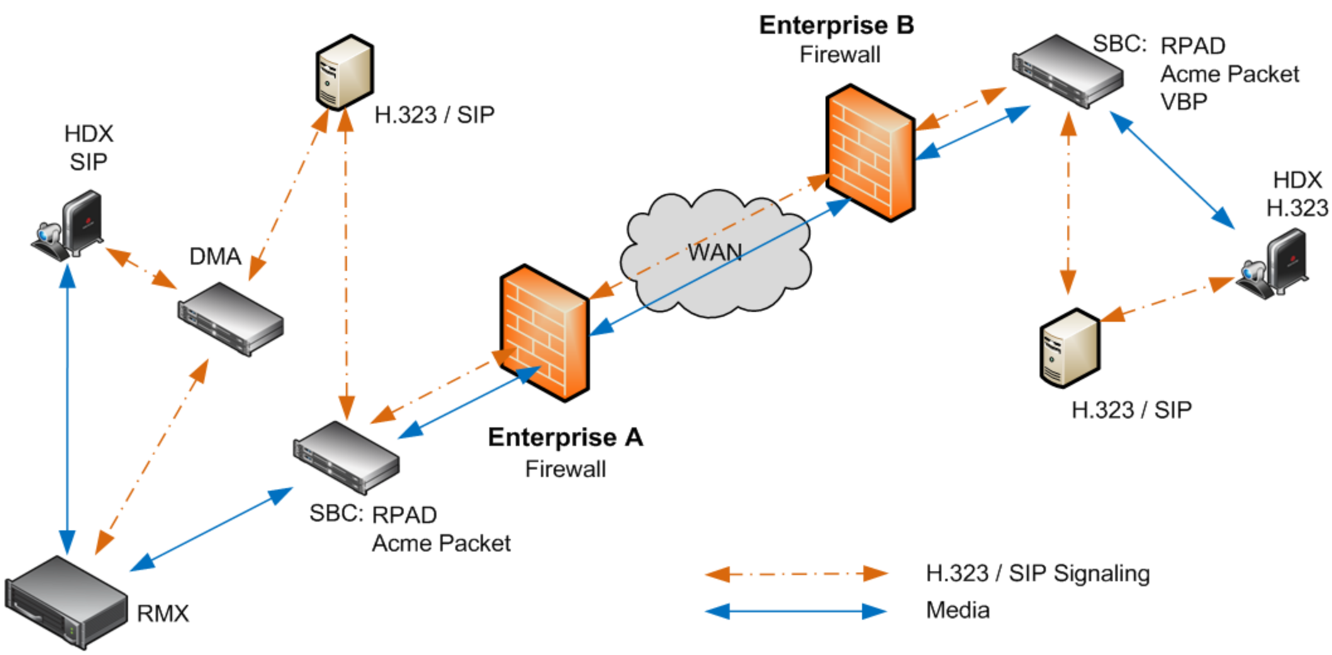
Table 16-40 *Remote Connection*

Enterprise Client				CMA Client	
Environment	Registered	SBC		Registered	Environment
SIP / H.323	Yes	SAM / Acme Packet	⇆	Yes	SIP
SIP / H.323	No	SAM / Acme Packet	⇆	No	SIP

Table 16-40 Remote Connection (Continued)

Enterprise Client				CMA Client	
Environment	Registered	SBC		Registered	Environment
SIP / H.323	No	SAM Only	⇆	No	H.323

Business to Business Connections



The following *Business to Business* connection call flow options are supported:

Table 16-41 Business to Business Connection

Enterprise A Client				Enterprise B Client		
Environment	Registered	SBC		SBC	Registered	Environment
H.323	Yes	RPAD	⇆	RPAD	Yes	H.323
H.323	Yes	RPAD	⇆	VBP	Yes	H.323
SIP	Yes	RPAD	⇆	RPAD	Yes	H.323
SIP	Yes	Acme Packet	⇆	Acme Packet	Yes	H.323

FW (Firewall) NAT Keep Alive

The RMX can be configured to send a *FW NAT keep alive* message at specific *Intervals* for the *RTP, UDP* and *BFCP* channels.

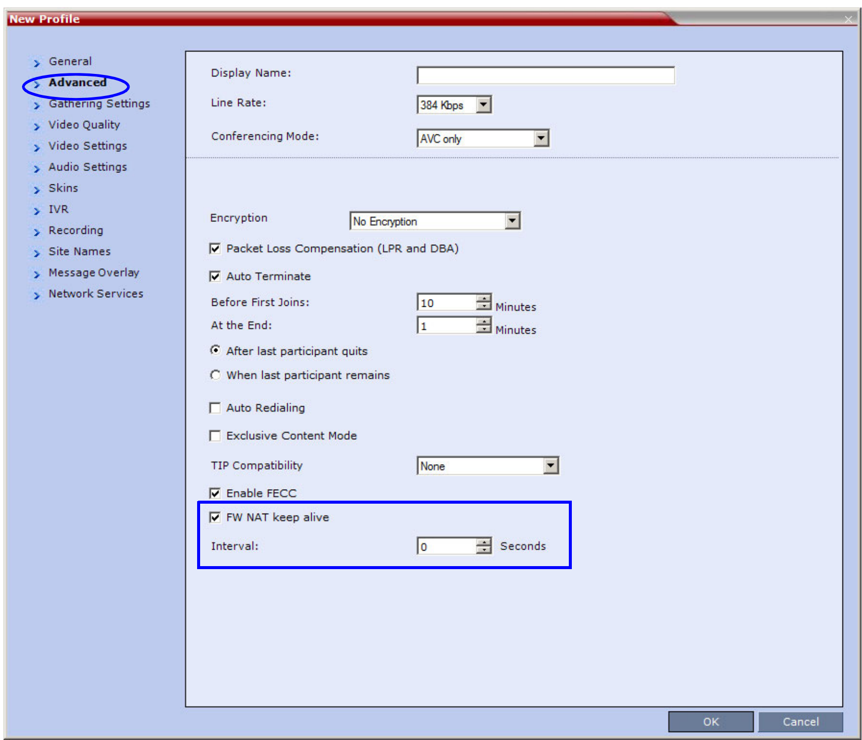
This is necessary because port mappings in the firewall are kept open only if there is network traffic in both directions. The firewall will only allow *UDP* packets into the network through ports that have been used to send packets out.

By default the RMX sends a *FW NAT Keep Alive* message every **30** seconds. As there is no traffic on the *Content* and *FECC* channels as a call begins, the firewall will not allow any incoming packets from the *Content* and *FECC* channels in until the RMX sends out the first of the *FW NAT Keep Alive* messages 30 seconds after the call starts.

If *Content* or *FECC* are required within the first 30 seconds of a call the *FW NAT Keep Alive Interval* should be modified to a lower value.

To enable and modify FW NAT Keep Alive:

FW NAT Keep Alive is enabled in the *New Profile - Advanced* dialog box.



>> Select the *FW NAT Keep Alive* check box and if required, modify the *Interval* field within the range of **5 - 86400** seconds.

System Configuration in SBC environments

In an environment that includes *SAM* (a *Polycom SBC*), to ensure that a *RealPresence Mobile* endpoint can send content to a conference the value of the system flag **NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT** must be set to at least 3.

For more details on modifying the values of system flags, see "*Manually Adding and Deleting System Flags"* on page 22-18.

17

IVR Services

> IVR Services are supported in AVC Conferencing Mode only.

Interactive Voice Response (IVR) is an application that allows participants to communicate with the conferencing system via their endpoint's input device (such as a remote control). The IVR Service includes a set of voice prompts and a video slide used to automate the participants connection to a conference or Entry Queue. It allows customization of menu driven scripts and voice prompts to meet different needs and languages.

The IVR module includes two types of services:

- Conference IVR Service that is used with conferences
- Entry Queue IVR Service that is used with Entry Queues

The system is shipped with two default Conference IVR Services (one for the conferences and the other for gateway calls) and one default Entry Queue IVR Service. The default services include voice messages and video slides in English.

To customize the IVR messages and video slide perform the following operations:

- Record the required voice messages and create a new video slide. For more information, see "*Creating a Welcome Video Slide"* on page **17-32**.
- Optional. Add the language to the list of languages supported by the system.
- Upload the voice messages to the MCU (This can be done as part of the language definition or during the IVR Service definition).
- Create the Conference IVR Service and upload the video slide, and if required any additional voice messages.
- Optional. Create the Entry Queue IVR Service and upload the required video slide and voice messages.

> When upgrading the RMX software version new DTMF Codes and voice messages are not automatically added to existing IVR Services in order to avoid conflicts with existing DTMF codes. Therefore, to use new options, new Conference and Entry Queue IVR Services must be created.

IVR Services List

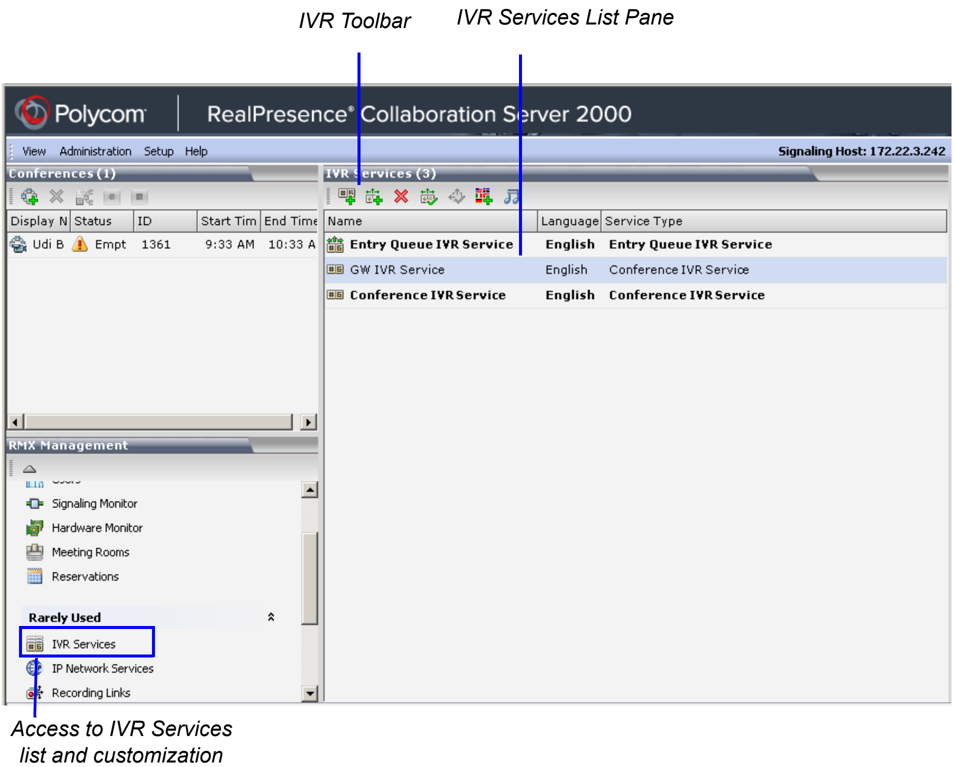
You can view the currently defined Conference IVR and Entry Queue IVR Services in the *IVR Services* list pane.

To view the IVR Services list:

1 In the *RMX Management* pane, expand the *Rarely Used* list.

2 Click the **IVR Services** ( ) entry.

The list pane displays the *Conference IVR Services* list and the total number of IVR services currently defined in the system.



IVR Services Toolbar

The IVR Services toolbar provides quick access to the IVR Service definitions as follows:

Table 17-1 *IVR Toolbar buttons*

Button	Button Name	Descriptions
	*New Conference IVR Service*	To create a new Conference IVR Service.
	*New Entry Queue IVR Service*	To create a new Entry Queue IVR Service.
	*Delete Service*	Deletes the selected IVR service(s).
	*Set Default Conference IVR Service*	Sets the selected Conference IVR Service as default. When creating a new conference Profile the default IVR Service is automatically selected for the Profile (but can be modified).
	*Set Default Entry Queue Service*	Sets the selected Entry Queue IVR Service as default. When creating a new Entry Queue the default Entry Queue IVR Service is automatically selected.

Table 17-1 *IVR Toolbar buttons*

Button	Button Name	Descriptions
	Add Supported Languages	Adds languages to the IVR module, enabling you to download voice prompts and messages for various languages.
	Replace/Change Music File	To replace the currently loaded music file that is used to play background music, the MCU is shipped with a default music file.

Adding Languages

You can define different sets of audio prompts in different languages, allowing the participants to hear the messages in their preferred language.

The RMX is shipped with a default language (English) and all the prompts and messages required for the default IVR Services, conference and Entry Queues shipped with the system.

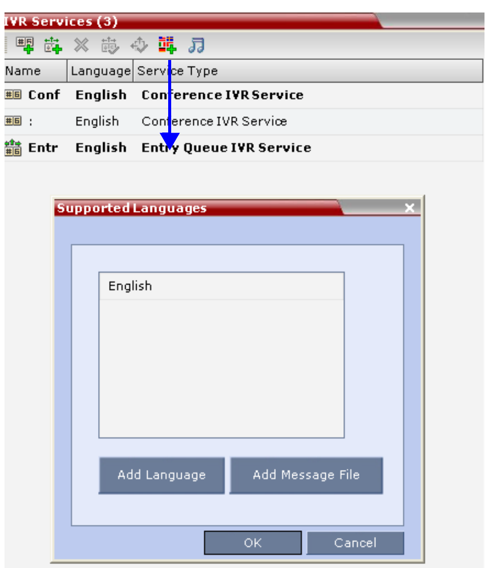
You can add languages to the list of languages for which different messages are downloaded to the MCU and IVR Services are created. This step is required before the creation of additional IVR messages using languages that are different from English, or if you want to download additional voice files to existing files in one operation and not during the IVR service definition.

To add a language:

1 In the *RMX Management* pane, expand the **Rarely Used** list.

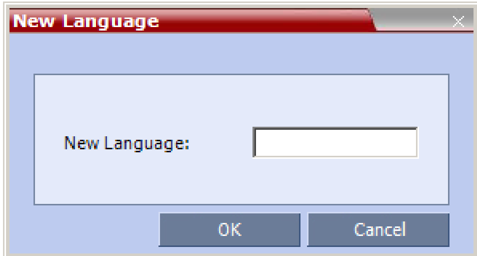
2 Click the **IVR Services** ( ) entry.

3 In the *Conference IVR Services* list, click the **Add Supported Languages** ( ) button. The *Supported Languages* dialog box opens.



4 Click the **Add Language** button.

The *New Language* dialog box opens.



5 In the *New Language* box, enter the name of the new language. The language name can be typed in Unicode and cannot start with a digit. Maximum field length is 31 characters.

6 Click **OK**.
The new language is added to the list of *Supported Languages*.

Uploading a Message File to the RMX

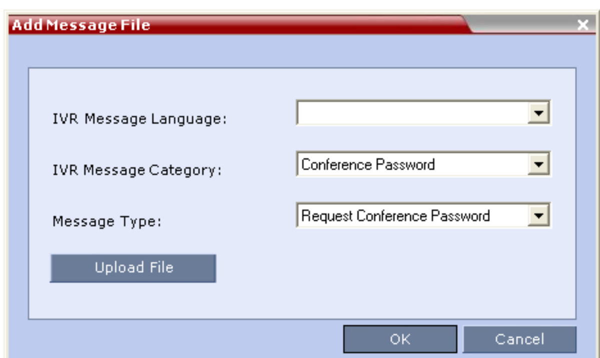
You can upload audio files for the new language or additional files for an existing language now, or you can do it during the definition of the IVR Service. In the latter case, you can skip the next steps.

- Voice messages should not exceed 3 minutes.
- It is not recommended to upload more than 1000 audio files to the MCU memory.

To upload messages to the MCU:

1 To upload the files to the MCU, in the *Supported Languages* dialog box, click the **Add Message File** button.

2 The *Add Message File* dialog box opens.



Audio files are uploaded to the MCU one-by-one.

3 In the *IVR Message Language* list, select the language for which the audio file will be uploaded to the MCU.

4 In the *IVR Message Category* list, select the category for which the audio file is uploaded.

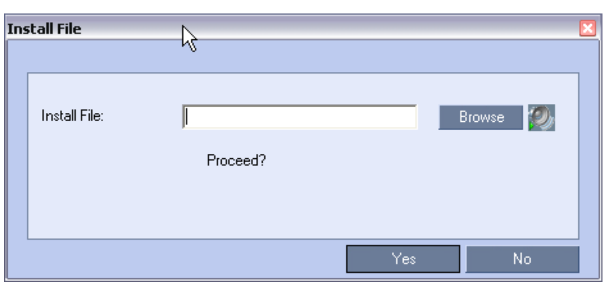
5 In the *Message Type* list, select the message type for which the uploaded message is to be played. You can upload several audio files for each Message Type. Each file is downloaded separately.

Table 17-2 lists the Message Types for each category:

Table 17-2 *IVR Message Types by Message Category*

Message Category	Message Type	Message
Conference Password	Request Conference Password	Requests the participant to enter the conference password.
	Request Conference Password Retry	A participant who enters an incorrect password is requested to enter it again.
	Request Digit	Requests the participant to enter any digit in order to connect to the conference. Used for dial-out participants to avoid answering machines in the conference.
Welcome Message	Welcome Message	The first message played when the participant connects to the conference or Entry Queue.
Conference Chairperson	Request Chairperson Identifier	Requests the participants to enter the chairperson identifier key.
	Request Chairperson Password	Requests the participant to enter the chairperson password.
	Request Chairperson Password Retry	When the participant enters an incorrect chairperson password, requests the participant to enter it again.
General	Messages played for system related event notifications, for example, notification that the conference is locked. Upload the files for the voice messages that are played when an event occurs during the conference. For more information, see "*Conference IVR Service Properties - General Voice Messages"* on page **17-11**.	
Billing Code	Requests the chairperson to enter the conference Billing Code.	
Roll Call	Roll call related messages, such as the message played when a participant joins the conference. Messages are listed in the *Conference IVR Service - Roll Call* dialog box.	
Conference ID	Requests the participant to enter the required Conference ID to be routed to the destination conference.	

6 Click **Upload File** to upload the appropriate audio file to the MCU.
The *Install File* dialog box opens.



7 Enter the file name or click the **Browse** button to select the audio file to upload.
The *Select Source File* dialog box opens.

8 Select the appropriate *.wav audio file, and then click the **Open** button.
The name of the selected file is displayed in the *Install* field in the *Install File* dialog box.

9 Optional. You can play a .wav file by selecting the *Play* button ( ).

10 Click **Yes** to upload the file to the MCU.
The system returns to the *Add Message File* dialog box.

11 Repeat step 6 to 10 for each additional audio file to be uploaded to the MCU.

12 Once all the audio files are uploaded to the MCU, close the *Add Message File* dialog box and return to the *Add Language* dialog box.

13 Click **OK**.

Defining a New Conference IVR Service

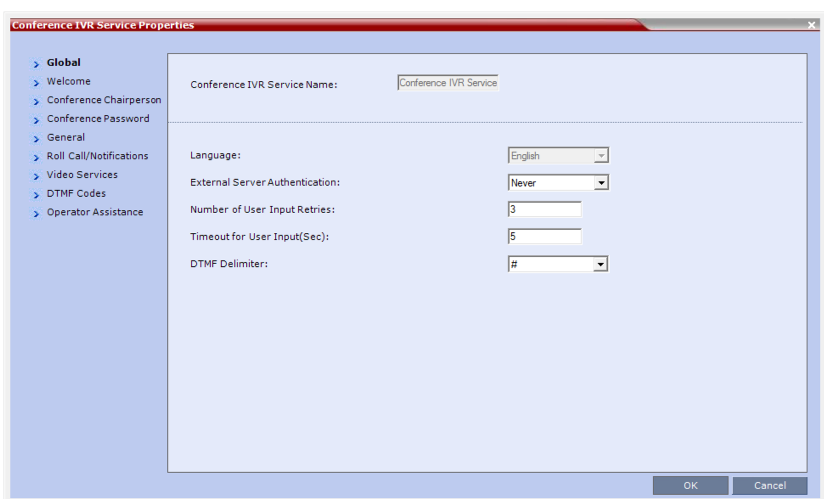
The RMX is shipped with two default Conference IVR Services and all its audio messages and video slide. You can define new Conference IVR Services or modify the default Conference IVR Service. For the definition of Conference IVR Service for gateway calls, see "*Defining the IVR Service for Gateway Calls"* on page **19-14**.

> Up to 40 IVR Services (Conference IVR Services and Entry Queue IVR Services) can be defined for a single RMX unit.

Defining a New Conference IVR Service

To define a new Conference IVR Service:

1 On the *IVR Services* toolbar, click the **New Conference IVR Service** ( ) button.
The *New Conference IVR Service - Global* dialog box opens.

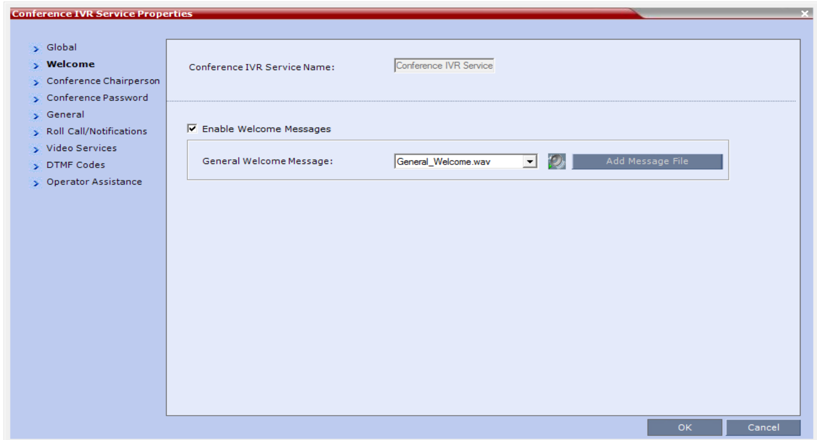


2 Define the following parameters:

Table 17-3 *Conference IVR Service Properties - Global Parameters*

Field/Option	Description
Conference IVR Service Name	Enter the name of the Conference IVR Service. The maximum field length is 20 characters and may be typed in Unicode.
Language For IVR	Select the language of the audio messages and prompts from the list of languages defined in the *Supported languages*. The default language is English. For more information, see "*Adding Languages"* on page **17-3**.
External Server Authentication	You can configure the IVR Service to use an external database application to verify a participant's right to join the conference. For more information, see *Appendix D:* "*Conference Access with External Database Authentication"* on page **D-4**. Select one of the following options: • ***Never*** – The participant's right to join the conference will not be verified with an external database application (default). • ***Always*** – Any participant request to join the conference is validated with the external database application using a password. • ***Upon Request*** – Only the participant request to join the conference as chairperson is validated with the external database application using a password. The validation process occurs only when the participant enters the chairperson identifier key.
Number of User Input Retries	Enter the number of times the participant will be able to respond to each menu prompt before being disconnected from the conference. Range is between 1-4, and the default is 3.
Timeout for User Input (Sec)	Enter the duration in seconds that the system will wait for the participant's input before prompting for another input. Range is between 1-10, and the default value is 5 seconds.
DTMF Delimiter	Enter the key that indicates the last input key. Possible values are the pound (#) and star (*) keys. The default is #.

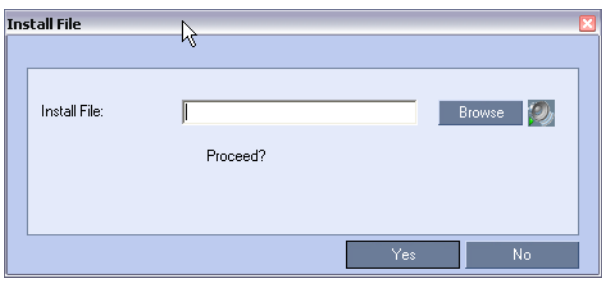
3 Click the **Welcome** tab.
The *New Conference IVR Service - Welcome* dialog box opens.



4 Select the **Enable Welcome Messages** check box to define the system behavior when the participant enters the Conference IVR queue. When participants access a conference through an Entry Queue, they hear messages included in both the Entry Queue Service and Conference IVR Service. To avoid playing the Welcome Message twice, disable the Welcome Message in the Conference IVR Service.

5 Select the **General Welcome Message,** to be played when the participant enters the conference IVR queue.

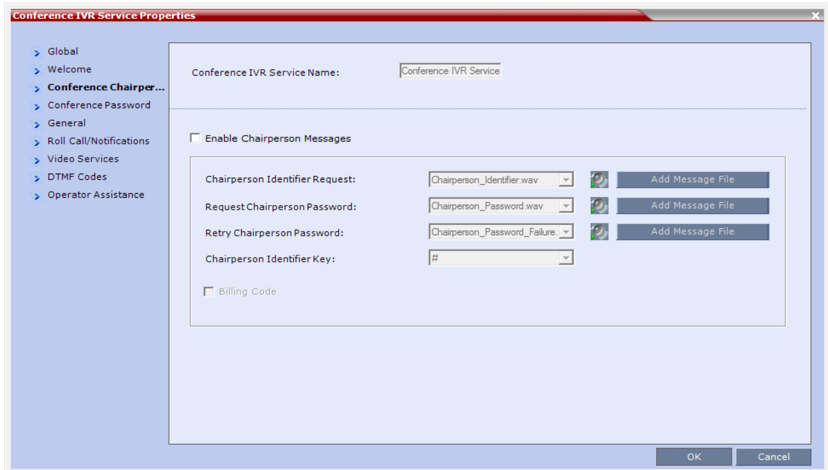
6 To upload an audio file for an IVR message, click **Add Message File**.
The *Install File* dialog box opens.



> The RMX unit is bundled with default audio IVR message files. To upload a customized audio file, see *"Creating Audio Prompts and Video Slides"* on page **17-28**.

- **a** Click the **Browse** button to select the audio file (*.wav) to upload.
  The *Select Source File* dialog box opens.
- **b** Select the appropriate *.wav audio file and then click the **Open** button.
- **c** Optional. You can play a .wav file by selecting the *Play* button ( ).
- **d** In the *Install File* dialog box, click **Yes** to upload the file to the MCU memory.
  The *Done* dialog box opens.
- **e** Once the upload is complete, click **OK** and return to the *IVR* dialog box. The new audio file can now be selected from the list of audio messages.

7 Click the **Conference Chairperson** tab.
The *New Conference IVR Service - Conference Chairperson* dialog box opens.



8 Select the **Enable Chairperson Messages** check box to enable the chairperson functionality. If this feature is disabled, participants are not able to connect as the chairperson.

> When both Conference Password and Chairperson Password options are enabled and defined, the system first plays the prompt "Enter conference password". However, if the participant enters the chairperson password, the participant becomes the chairperson.
> To play the prompt requesting the Chairperson password, "For conference chairperson services...", **do not select** the *Enable Password Messages* option.

9 Select the various voice messages and options for the chairperson connection.

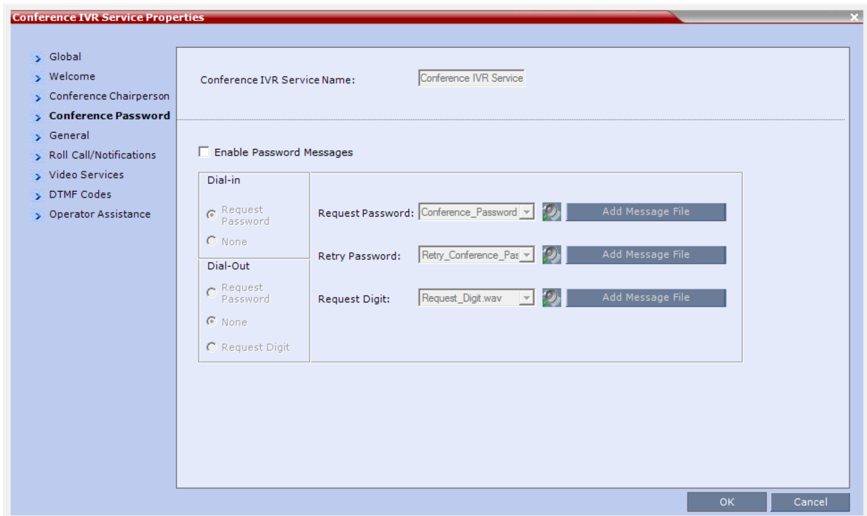
> If the files were not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the RMX.

Table 17-4 *New Conference IVR Service Properties - Conference Chairperson Options and Messages*

Field/Option	Description
Chairperson Identifier Request	Select the audio file that requests the participants to enter the key that identifies them as the conference chairperson.
Request Chairperson Password	Select the audio file that prompts the participant for the chairperson password.
Retry Chairperson Password	Select the audio file that prompts participants to re-enter the chairperson password if they enter it incorrectly.
Chairperson Identifier Key	Enter the key to be used for identifying the participant as a chairperson. Possible keys are: pound key (#) or star (*).
Billing Code	The prompt requesting the chairperson billing code selected in the General tab.

10 Click the **Conference Password** tab.

The *New Conference IVR Service - Conference Password* dialog box opens.



11 Select the **Enable Password Messages** check box to request the conference password before moving the participant from the conference IVR queue to the conference.

When both Conference Password and Chairperson Password are enabled and defined, the system first plays the prompt "Enter conference password". However, if the participant enters the chairperson password, the participant becomes the chairperson.
To play the prompt requesting the Chairperson password, "For conference chairperson services...", **do not select** the *Enable Password Messages* option.

12 Select the MCU behavior for password request for *Dial-in* and *Dial-out* participant connections.

Select the required system behavior as follows:

— **Request password** - The system requests the participant to enter the conference password.

— **None** - The participant is moved to the conference without any password request.

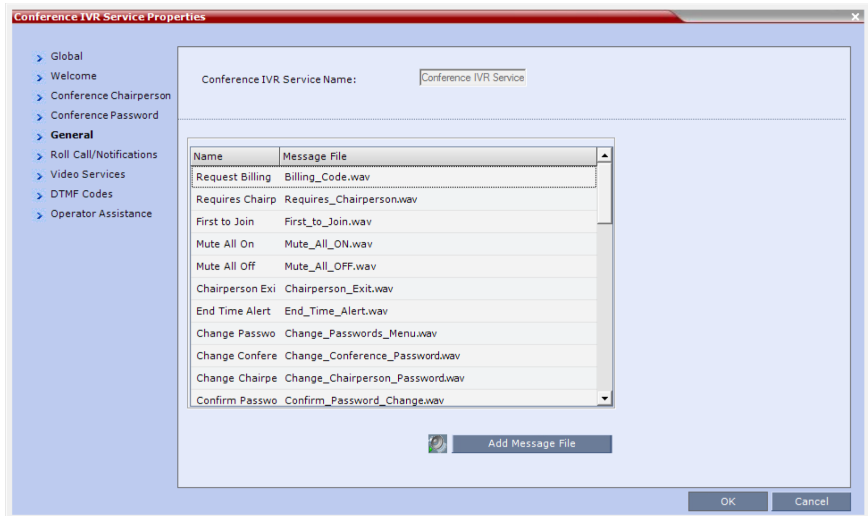
— **Request Digit** - The system requests the participant to enter any key. This option is used mainly for dial-out participants and to prevent an answering machine from entering the conference.

13 Select the various audio messages that will be played in each case.

Table 17-5 *New Conference IVR Service Properties - Conference Password Parameters*

Option	Description
Request Password	Select the audio file that prompts the participant for the conference password.
Retry Password	Select the audio file that requests the participant to enter the conference password again when failing to enter the correct password.
Request Digit	Select the audio file that prompts the participant to press any key when the *Request Digit* option is selected.

14 Click the **General** tab.
The *New Conference IVR Service - General* dialog box opens.



The *General* dialog box lists messages that are played during the conference. These messages are played when participants or the conference chairperson perform various operations or when a change occurs.

15 To assign the appropriate audio file to the message type, click the appropriate table entry, in the *Message File* column. A drop-down list is enabled.

16 From the list, select the audio file to be assigned to the event/indication.

17 Repeat steps 15 and 16 to select the audio files for the required messages.
The following types of messages and prompts can be enabled:

Table 17-6 *Conference IVR Service Properties - General Voice Messages*

Message Type	Description
Blip on Cascade Link	Indicates that the link to the cascaded conference connected successfully.
Chairperson Exit	Informs all the conference participants that the chairperson has left the conference, causing the conference to automatically terminate after a short interval. **Note:** This message is played only when the *Requires Chairperson* option is selected in the *Conference Profile - IVR* dialog box.
Chairperson Help Menu	A voice menu is played upon a request from the chairperson, listing the operations and their respective DTMF codes that can be performed by the chairperson. The playback can be stopped any time. **Note:** If you modify the default DTMF codes used to perform various operations, the default voice files for the help menus must be replaced.
Change Chairperson Password	Requests the participant to enter a new chairperson password when the participant is attempting to modify the chairperson password.
Change Conference Password	Requests the participant to enter a new conference password when the participant is attempting to modify the conference password.

Table 17-6 *Conference IVR Service Properties - General Voice Messages (Continued)*

Message Type	Description
Change Password Failure	A message played when the participant enters an invalid password, for example when a password is already in use.
Change Passwords Menu	This voice menu is played when the participants requests to change the conference password. This message details the steps required to complete the procedure.
Conference is Locked	This message is played to participants attempting to join a Secured conference.
Conference is Secured	This message is played when the conference status changes to Secure as initiated by the conference chairperson or participant (using DTMF code *71).
Conference is unsecured	This message is played when the conference status changes to Unsecured as initiated by the conference chairperson or participant (using DTMF code #71).
Confirm Password Change	Requests the participant to re-enter the new password.
Dial Tone	The tone that will be played to indicate a dialing tone, to let the calling participant enter the destination number.
Disconnect on Busy	The *Busy Tone* is played when the system retries to redial a busy destination number and fails after exceeding the number of redials. This call is then disconnected.
Disconnect on No Answer	The *Reorder Tone* is played when the system retries to redial a destination number that does not answer and fails after exceeding the number of redials. This call is then disconnected.
Disconnect on Wrong Number	A voice message is played when the call fails because of an incorrect destination number. The message is followed the *Reorder Tone* and the call is disconnected.
End Time Alert	Indicates that the conference is about to end.
Enter Destination ID	Prompts the calling participant for the destination number. Default message prompts the participant for the conference ID (same message as in the Entry Queue IVR Service).
First to Join	Informs the participant that he or she is the first person to join the conference.
Incorrect Destination ID	If the participant entered an incorrect conference ID (in gateway calls it is the destination number), requests the participant to enter the number again.
Maximum Number of Participants Exceeded	Indicates the participant cannot join the destination conference as the maximum allowed number of participants will be exceeded.
Mute All Off	This message is played to the conference to inform all participants that they are unmuted (when *Mute All* is cancelled).

Table 17-6 *Conference IVR Service Properties - General Voice Messages (Continued)*

Message Type	Description
Mute All On	Informs all participants that they are muted, with the exception of the conference chairperson. **Note:** This message is played only when the *Mute All Except Me* option is activated.
No Video Resources Audio Only.	Informs the participant of the lack of Video Resources in the RMX and that he/she is being connected as Audio Only.
Participant Help Menu	A voice menu that is played upon request from a participant, listing the operations and their DTMF codes that can be performed by any participant.
Password Changed Successfully	A message is played when the password was successfully changed.
Recording Failed	This message is played when the conference recording initiated by the chairperson or the participant (depending on the configuration) fails to start.
Recording in Progress	This message is played to participant joining a conference that is being recorded indicating the recording status of the conference.
Redial on Wrong Number	A message is played requesting the participant to enter a new destination number followed by up to five redial attempts. If all redial attempts fail, the participant is alerted by an IVR message that the dialed number is unreachable, followed by the *Reorder Tone* and disconnection.
Request Billing Code	Requests the participant to enter a code for billing purposes.
Requires Chairperson	The message is played when the conference is on hold and the chairperson joins the conference. For this message to be played the *Conference Requires Chairperson* option must be selected in the *Conference Profile - IVR* dialog box.
Ringing Tone	The tone that will be played to indicate that the system is calling the destination number.
Self Mute	A confirmation message that is played when participants request to mute their line.
Self Unmute	A confirmation message that is played when participants request to unmute their line.

18 Click the **Roll Call** tab.
The *New Conference IVR Service - Roll Call* dialog box opens.

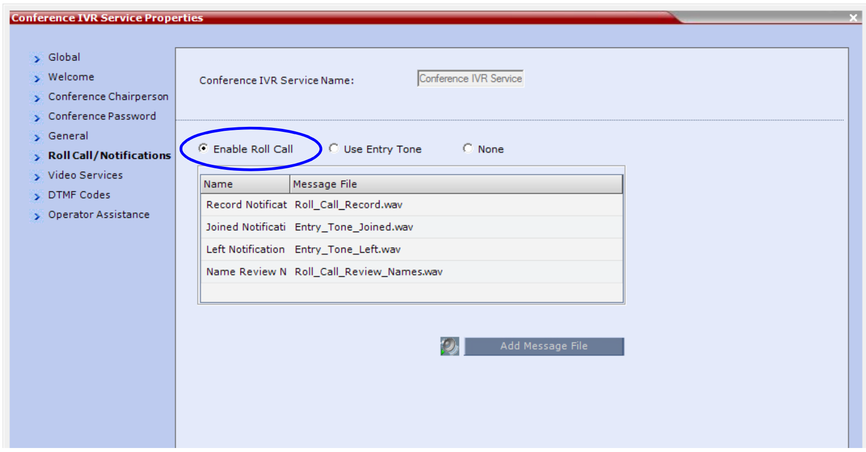
The Roll Call feature of the Conference IVR Service is used to record the participants' names for playback when the participants join and leave a conference.

Roll Call announcements played upon a participant's connection or disconnection from a conference (Entry and Exit announcements) can be replaced by tones. These tones can be used as notification when participants join or leave the conference but the identification of the participant is not required. The system is shipped with two default tones: Entry Tone and Exit tone. When the Tone Notifications option is enabled, no recording of the participant names will occur and the conference chairperson will not be able to ask for a name review during the conference.

From version 7.6, the selection of tones in the IVR Service definition replaces the functionality of the system flag IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE.

19 Select one of the following options to determine the announcement mode:

a To enable the Roll Call feature, select the **Enable Roll Call** option.



b Select **Enable Tones** to enable the Tone Notifications option.
The dialog box changes to display the tone notification options and all Roll Call options are disabled. In such a case, skip to step 22.

c Select **None** to disable the Roll Call and Tone Notifications features.

If *Enable Roll Call* option is selected:

20 To assign the audio file to the message type, in the Message File column, click the appropriate table entry. An arrow appears in the *Message File* column.

> If the Roll Call option is enabled, you must assign the appropriate audio files to all message types.

21 Click the arrow to open the *Message File* list and select the appropriate audio file.

Table 17-7 Conference IVR Service Properties - Roll Call Messages

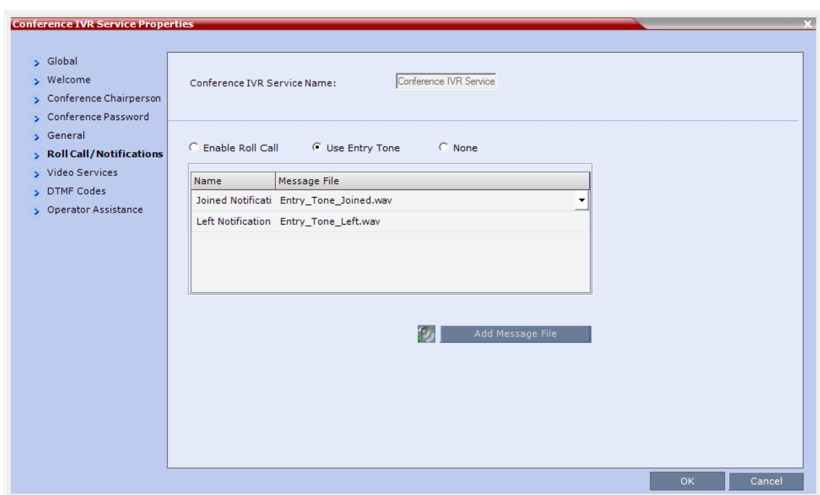
Roll Call Message	Description
Roll Call Record	Requests participants to state their name for recording, when they connect to the conference. **Note:** The recording is automatically terminated after two seconds.

Table 17-7 Conference IVR Service Properties - Roll Call Messages (Continued)

Roll Call Message	Description
Roll Call Joined	A voice message stating that the participant has joined the conference. **Note:** In versions prior to 7.6, when the system flag *IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE* is set to **YES**, the system does not playback the Roll Call names when participants enter the conference. However, the voice message will be played, unless it is replaced with tone file. In such a case, the use of tones requires the uploading of the appropriate tone files in *.wav format and replacing the Roll Call Joined message file with the tone file.
Roll Call Left	A voice message stating that the participant has left the conference. **Note:** In versions prior to 7.6, when the system flag *IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE* is set to **YES**, the system does not playback the Roll Call names when participants exit the conference. However, the voice message will be played, unless it is replaced with tone file. In such a case, the use of tones requires the uploading of the appropriate tone files in *.wav format and replacing the Roll Call Left message file with the tone file.
Roll Call Review	Played when Roll Call is requested by the chairperson, introducing the names of the conference participants in the order they joined the conference.

If *Enable Tone Notifications* option is selected:

22 Select the Entry Tone or Exit tone:



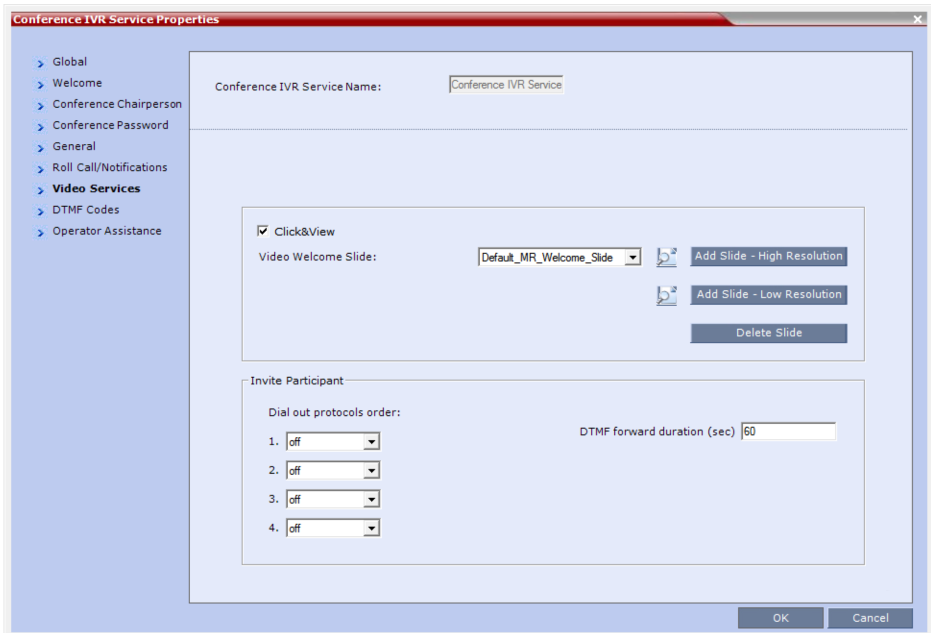
a Click the appropriate table entry in the *Message File* column.
A drop-down list is enabled.

b From the list, select the audio file to be assigned to the event/indication.

> If the Tones option is enabled, you must assign the appropriate audio files to all notification types.
> The RMX system is shipped with two default tones: Entry_tone.wav and Exit_tone.wav.
> If required, you can upload customized audio files that will be played when participants join or leave the conference.
>
> If the option to play a tone when a cascading link connection is established, make sure that the tone selected for Entry or Exit notification differ from the cascading link tone as the latter one cannot be customized.

23 Click the **Video Services** tab.

The *New Conference IVR Service - Video Services* dialog box opens.



In addition to the low and high resolution slides included in the default slide set, customized low and high resolution slides are supported.

The following guidelines apply:

— Two customized slides can be loaded per *IVR Service*:
  - A low resolution slide, to be used with low resolution endpoints.
  - A high resolution slide, to be used with high resolution endpoints.

  Table 17-8 summarizes the recommended input slide formats and the resulting slides that are generated:

Table 17-8 *IVR Slide - Input / Output Formats*

Slide Resolution	Format	
	Input Slides	**Generated Slides**
High	HD1080p (16:9) or HD720p (16:9)	HD1080p HD720p

Table 17-8 IVR Slide - Input / Output Formats (Continued)

Slide Resolution	Format	
	Input Slides	Generated Slides
Low	4CIF (4:3) or CIF (4:3)	4SIF SIF CIF

— The source images for the high resolution slides must be in ***.bmp*** or ***.jpg*** format.
— If the uploaded slides are not of the exact *SD* or *HD* resolution, an error message is displayed and the slides are automatically cropped or enlarged to the right size.
— If a slide that is selected in an *IVR Service* is deleted, a warning is displayed listing the *IVR Services* in which it is selected. If deleted, it will be replaced with a default RMX slide.
— The generated slides are not deleted if the system is downgraded to a lower software version.
— The first custom source file uploaded, whatever its format, is used to generate both high and low resolution custom slides. High resolution source files uploaded after the first upload will be used to generate and replace high resolution custom slides. Likewise, low resolution source files uploaded after the first upload will be used to generate and replace low resolution custom slides.
— If there are two custom source files in the folder, one high resolution, one low resolution, and a new high resolution custom source file is uploaded, new high resolution custom slides are created. The existing low resolution custom slides are not deleted.
— If there are two custom source files in the folder, one high resolution, one low resolution, and a new low resolution custom source file is uploaded, new low resolution custom slides are created. The existing high resolution custom slides are not deleted.

24 Define the following parameters:

Table 17-9 New Conference IVR Service Properties - Video Services Parameters

Video Services	Description
Click&View	Select this option to enable endpoints to run the Click&View application that enables participants to select a video layout from their endpoint.
Video Welcome Slide	Select the *Low Resolution* and *High Resolution* video slides to be displayed when participants connect to the conference. To view any slide, click the **Preview Slide** ( ) button. **Notes:** • When using one of the default Polycom slides, the slide will be displayed in the resolution defined in the profile, i.e. CIF, SD, HD 720p or HD 1080p. When defining a gateway IVR Service, the recommended default slide is: Default_GW_Welcome_Slide. • Customized H.261 slides are not supported. • When RMX is configured to IPv6, the IVR slide is displayed without taking into account the MTU Size.

Table 17-9 *New Conference IVR Service Properties - Video Services Parameters (Continued)*

Video Services	Description
Invite Participant	See *"Inviting Participants using DTMF"* **on page 17-33.**
Dial out protocols order	Select the order of the network protocols that will be used by the system to dial the destination number. The system will start dialing using the first protocol, and if the call is not answered it will continue with the second, third and fourth protocols (if they are enabled) until the call is answered. By default, H.323 is set as the first protocol and SIP as the second while the remaining protocols are disabled (set to Off). For PSTN calls, select the PSTN protocol and not ISDN. Set PSTN before ISDN if both PSTN and ISDN protocols are required.
DTMF forward duration	Use this field when connecting to another conferencing entity with an IVR, requiring the input of a password, destination number or ID. Enter the number of seconds that the system will wait for the input of additional DTMF digits such as a password or conference number. Range: 10 - 600 seconds Default: 60 seconds.

25 If the video slide file was not uploaded to the MCU prior to the IVR Service definition, click the:

— **Add Slide - Low Resolution** button to upload a *Low Resolution Slide*.

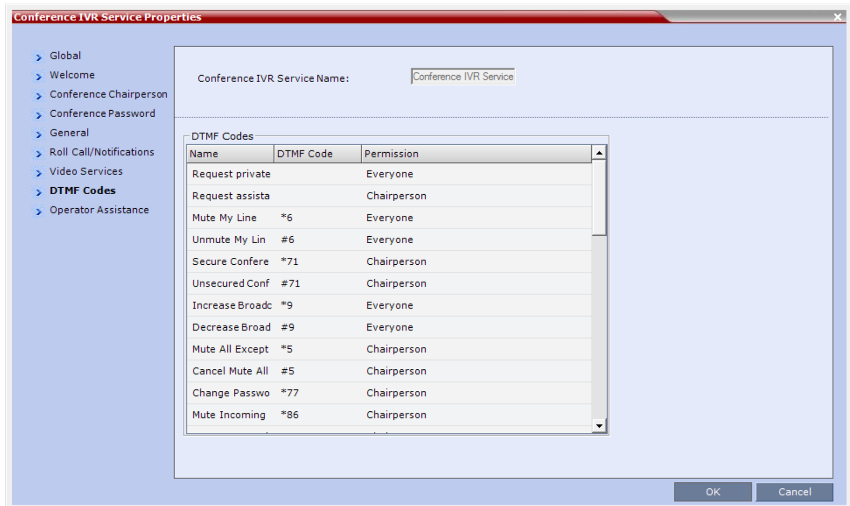
— **Add Slide - High Resolution** button to upload a *High Resolution Slide*.

The *Install File* dialog box opens. The uploading process is similar to the uploading of audio files. For more information, see step **6** on page 17-8.

- The video slide must be in a .jpg or .bmp file format. For more information, see "*Creating a Welcome Video Slide"* on page 17-32.
- Customized H.261 slides are not supported.

26 Click the **DTMF Codes** tab.

The *New Conference IVR Service - DTMF Codes* dialog box opens.



- This dialog box lists the default DTMF codes for the various functions that can be performed during the conference by all participants or by the chairperson.

Table 17-10 New Conference IVR Service Properties - DTMF Codes

Operation	DTMF String	Permission
Mute My Line	*6	Everyone
Unmute My Line	#6	Everyone
Increase Broadcast Volume	*9	Everyone
Decrease Broadcast Volume	#9	Everyone
Mute All Except Me	*5	Chairperson
Cancel Mute All Except Me	#5	Chairperson
Change Password	*77	Chairperson
Mute Incoming Participants	*86	Chairperson
Unmute Incoming Participants	#86	Chairperson
Play Help Menu	*83	Everyone
Enable Roll Call	*42	Chairperson
Disable Roll Call	#42	Chairperson
Roll Call Review Names	*43	Chairperson
Roll Call Stop Review Names	#43	Chairperson
Terminate Conference	*87	Chairperson
Start Click&View	**	Everyone
Start PCM	##	Everyone

Table 17-10 New Conference IVR Service Properties - DTMF Codes

Operation	DTMF String	Permission
Invite Participant	*72	Everyone
Disconnect Last Invited Participant	#72	Chairperson
Change To Chairperson	*78	Everyone
Increase Listening Volume	*76	Everyone
Decrease Listening Volume	#76	Everyone
Override Mute All	Configurable	Everyone
Start Recording	*3	Chairperson
Stop Recording	*2	Chairperson
Pause Recording	*1	Chairperson
Secure Conference	*71	Chairperson
Unsecured Conference	#71	Chairperson
Show Number of Participants	*88	Everyone
Request individual assistance	*0	Everyone
Request assistance for conference	00	Chairperson
Request to Speak	99	Everyone
Touch Control Prefix	*#	Everyone

- Do not change the *DTMF* code of the **Touch Control Prefix** (***#**).
  The *Polycom® Touch Control* device is only supported with *MPM+* and *MPMx* media cards. For more information see the *Polycom® Touch Control User Guide*.
- If during the ongoing conference the S**how Number of Participants** DTMF option (default DTMF ***88**) is used, when the displayed number of participants is removed, the message overlay text is also removed.

27 To modify the DTMF code or permission:

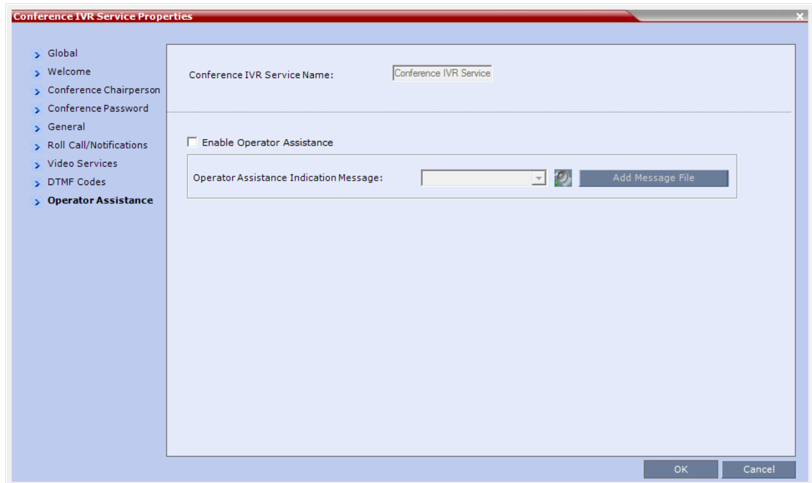
a In the *DTMF Code* column, in the appropriate entry enter the new code.

b In the *Permission* column, select from the list who can use this feature (Everyone or just the Chairperson).

By default, the Secure, Unsecure Conference and Show Number of Participants options are enabled in the Conference IVR Service. These options can be disabled by removing their codes from the Conference IVR Service.

- To disable the Secure Conference options, in the *DTMF Code* column, clear the DTMF codes of both Secured Conference **(*71)** and Unsecured Conference **(#71)** from the table.
- To disable the Text Indication option in the DTMF Code column, clear the DTMF code **(*88)** of *Show Number of Participants* from the table.

28 Click the **Operator Assistance** tab.
The *Operator Assistance* dialog box opens.



29 Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process to the conference or during the conference.

30 In the *Operator Assistance Indication Message* field, select the audio message to be played when the participant requests or is waiting for the operator's assistance.

> If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the RMX.

31 Click **OK** to complete the IVR Service definition.
The new Conference IVR Service is added to the *IVR Services* list.

Entry Queue IVR Service

An Entry Queue (EQ) is a routing lobby for conferences. Participants are routed to the appropriate conference according to the conference ID they enter.

An Entry Queue IVR Service must be assigned to the Entry Queue to enable the voice prompts and video slide guiding the participants through the connection process.

An Entry Queue IVR Service is a subset of an IVR Service. You can create different Entry Queue Services for different languages and personalized voice messages.

The RMX is shipped with a default Entry Queue IVR Service and all its audio messages and video slide. You can define new Entry Queue IVR Services or modify the default Entry Queue IVR Service.

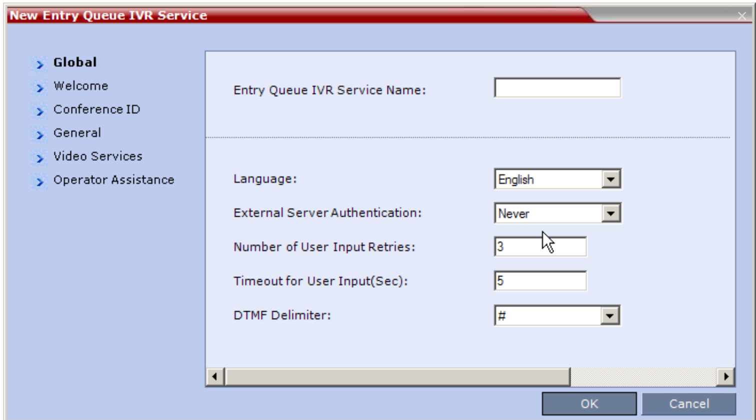
Defining a New Entry Queue IVR Service

To set up a new Entry Queue IVR Service:

1 In the *RMX Management* pane, click **IVR Services** ( ).

2 In the *IVR Services* list, click the **New Entry Queue IVR Service** (*)* button.

The *New Entry Queue IVR Service - Global* dialog box opens.

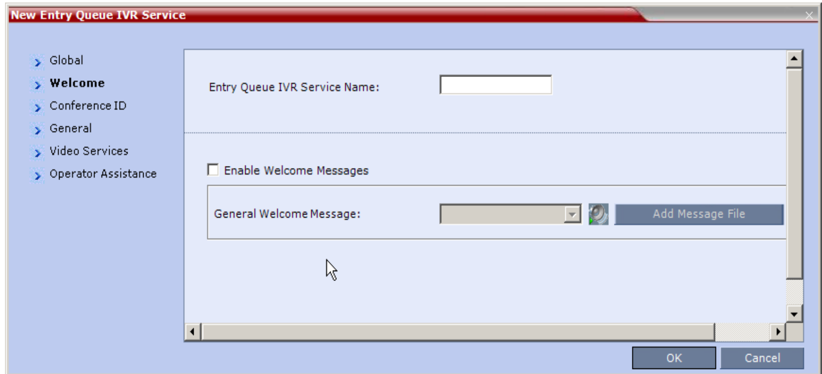


3 Fill in the following parameters:

Table 17-11 *Entry Queue IVR Service Properties - Global Parameters*

Option	Description
Entry Queue Service Name	(Mandatory) Enter the name of the Entry Queue Service. The name can be typed in Unicode. Maximum field length is 80 ASCII characters.
Language	Select the language in which the Audio Messages and prompts will be heard. The languages are defined in the *Supported Languages* function.
External Server Authentication	This option is used for Ad Hoc conferencing, to verify the participant's permission to initiate a new conference. For a detailed description see *Appendix D:* "*Conference Access with External Database Authentication"* on page **D-4**. Select one of the following options: • **None** to start a new conference without verifying with an external database the user right to start it. • **Conference ID** to verify the user's right to start a new conference with an external database application using the conference ID.
Number of User Input Retries	Enter the number of times the participant is able to respond to each menu prompt before the participant is disconnected from the MCU.
Timeout for User Input (Sec.)	Enter the duration in seconds that the system waits for input from the participant before it is considered as an input error.
DTMF Delimiter	The interaction between the caller and the system is done via touch-tone signals (DTMF codes). Enter the key that will be used to indicate a DTMF command sent by the participant or the conference chairperson. Possible keys are the pound key (#) or star (*).

4 Click the **Welcome** tab.
The *New Entry Queue IVR Service - Welcome* dialog box opens.

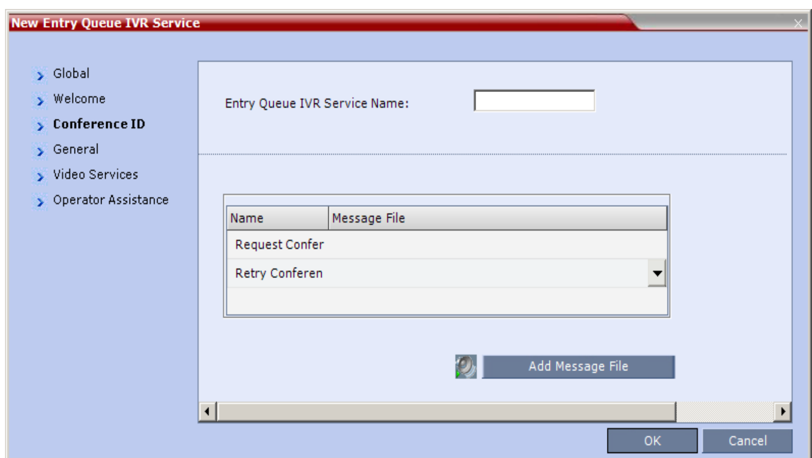


If the files were not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the RMX.

5 Define the appropriate parameters. This dialog box contains options that are identical to those in the *Conference IVR Service - Welcome Message* dialog box. For more information about these parameters, see Table 17-4 on page 17-9.

6 Click the **Conference ID** tab.

The *New Entry Queue IVR Service - Conference ID* dialog box opens.



7 Select the voice messages:

***Table 17-12** Entry Queue IVR Service Properties - Conference ID*

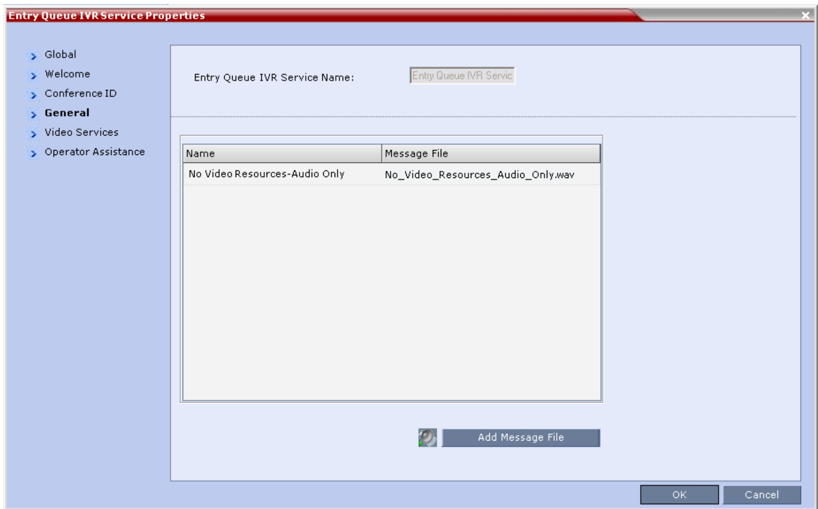
Field/Option	Description
Request Conference ID	Prompts the participant for the conference ID.
Retry Conference ID	When the participant entered an incorrect conference ID, requests the participant to enter the ID again.

8 Assign an audio file to each message type, as follows:

— In the *Message File* column, click the table entry, and then select the appropriate audio message.

9 Click the **General** tab.

The *New Entry Queue IVR Service - General* dialog box opens.



The administrator can enable an audio message that informs the participant of the lack of *Video Resources* in the RMX and that he/she is being connected as *Audio Only*. The message states: *All video resources are currently in use. Connecting using audio only*.

The following guidelines apply:

— The *IVR* message applies to video participants only. *Audio Only* participants will not receive the message.

— Only *H.323* and *SIP* participants receive the audio message.

— Downgrade to *Audio Only* is not supported for undefined *ISDN* dial in participants. These participants are disconnected if there is a lack of *Video Resources*.

— The audio message is the first message after the call is connected, preceding all other *IVR* messages.

— The message is called *No Video Resources-Audio Only* and the message file (*.wav*) is called *No video resources audio only.wav*.

— The audio message must be added to the *Conference* and *Entry Queue IVR Services* separately.

— The IVR message can be enabled/disabled by the administrator using the **ENABLE_ NO_VIDEO_RESOURCES_ AUDIO_ONLY_MESSAGE** *System Flag* in *system.cfg*.

Possible values: **YES** / **NO,** default: **YES**

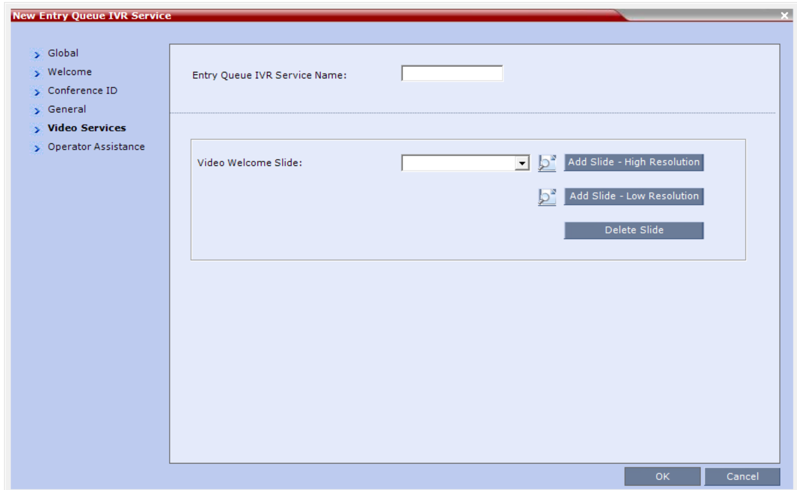
If you wish to modify the flag value, the flag must be added to the *System Configuration* file. For more information see the "*Modifying System Flags"* on page **22-1**.

10 Enter the message *Name* and *Message File* name for the *Audio Only* message:

— Message *Name*: **No Video Resources-Audio Only**

— *Message File* name: **No_Video_Resources_Audio_Only.wav**

11 Click the **Video Services** tab.
The *New Entry Queue IVR Service - Video Services* dialog box opens.



12 In the *Video Welcome Slide* list, select the video slide that will be displayed to participants connecting to the Entry Queue. The slide list includes the video slides that were previously uploaded to the MCU memory.

13 To view any slide, click the **Preview Slide** ( ) button.

14 If the video slide file was not uploaded to the MCU prior to the IVR Service definition, click the:

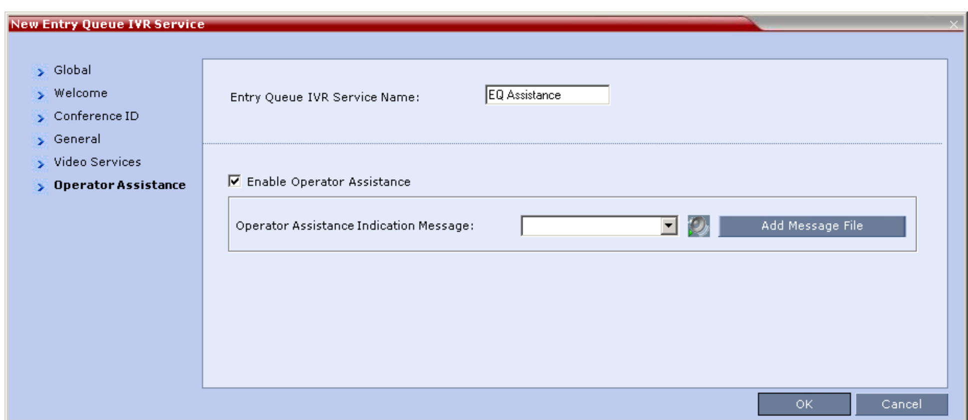
— **Add Slide - Low Resolution** button to upload a *Low Resolution Slide*.

— **Add Slide - High Resolution** button to upload a *High Resolution Slide*.

The *Install File* dialog box opens. The uploading process is similar to the uploading of audio files. For more information, see step **6** on page 17-8.

The video slide must be in a .jpg or .bmp file format. For more information, see "*Creating a Welcome Video Slide"* on page 17-32.

15 Click the **Operator Assistance** tab.
The *Operator Assistance* dialog box opens.



16 Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process.

17 In the *Operator Assistance Indication Message* field, select the audio message to be played when the participant requests or is waiting for operator's assistance.

> If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the RMX.

18 Click **OK** to complete the Entry Queue Service definition.
The new Entry Queue IVR Service is added to the *IVR Services* list. For more information, see "*IVR Services List*" on page **17-1**.

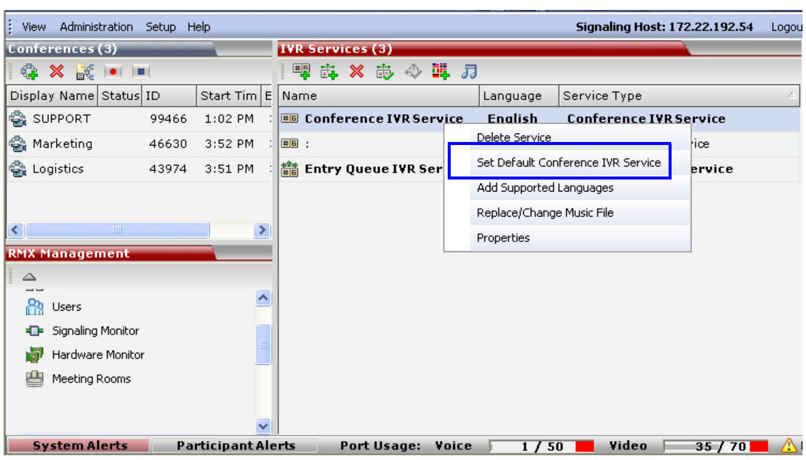
Setting a Conference IVR Service or Entry Queue IVR Service as the Default Service

The first Conference IVR Service and Entry Queue IVR Service are automatically selected by default. The IVR Services (Conference and Entry Queue) shipped with the system are also set as default. If additional Conference IVR Services and Entry Queue IVR Services are defined, you can set another service as the default for each service type.

To select the default Conference IVR Service:

>> In the *IVR Services* list, select the Conference IVR Service to be defined as the default, and then click the **Set Default Conference IVR Service** ( ) button.

Alternatively, in the *IVR Services* list, right-click the Conference IVR Service and then select *Set Default Conference IVR Service*.

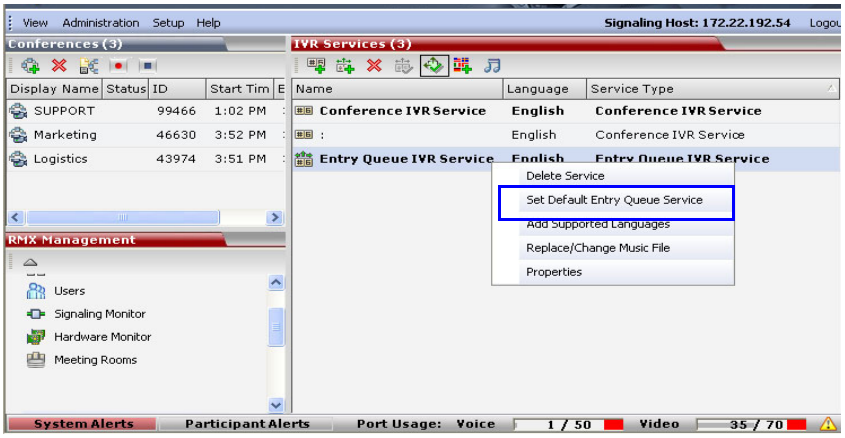


The IVR Service is displayed in bold, indicating that it is the current default service.

To select the Default Entry Queue IVR Service:

>> In the *IVR Services* list, select the Entry Queue IVR Service to be defined as the default, and then click **Set Default Entry Queue IVR Service** ( ) button.

Alternatively, in the *Conference IVR Services* list, right-click the Entry Queue IVR Service and then select *Set Default Entry Queue IVR Service*.



The default Entry Queue IVR Service is displayed in bold, indicating that it is the current default service.

Modifying the Conference or Entry Queue IVR Service Properties

You can modify the properties of an existing IVR Service, except the service name and language.

To modify the properties of an IVR Service:

1. In the *RMX Management* pane, click **IVR Services**.
2. In the *IVR Services* list, Click the IVR Service to modify.
   For more information about the tabs and options of this dialog box, see "*Defining a New Conference IVR Service"* on page 17-6.
3. Modify the required parameters or upload the required audio files.
4. Click **OK**.

Replacing the Music File

The RMX is shipped with a default music file that is played when participants are placed on hold, for example, while waiting for the chairperson to connect to the conference (if the conference requires a chairperson), or when a single participant is connected to the conference. You can replace the default music file with your own recorded music.

Music file guidelines:

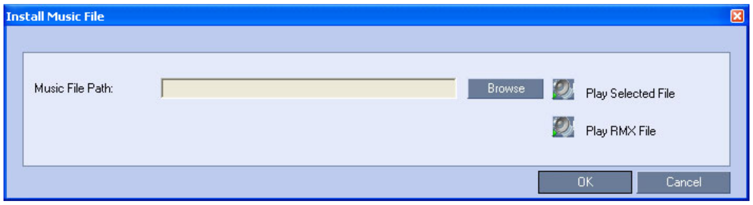
- The file must be in *.wav format.
- Music length cannot exceed one hour.
- The music recording must be in the range of (-12dB) to (-9dB).

Adding a Music File

To replace the Music file:

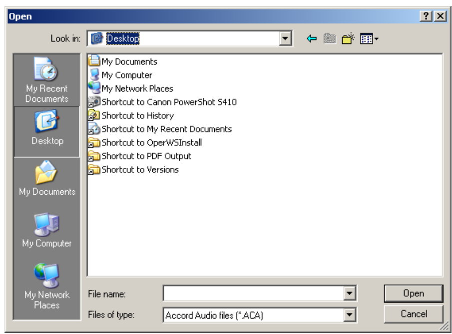
1. In the *RMX Management* pane, click **IVR Services**.

2 In the *IVR Services* list toolbar, click the **Replace/Change Music File** ( ) button.
The *Install Music File* window opens.



3 Click the **Browse** button to select the audio file (*.wav) to upload.

The *Open* dialog box opens.



4 Select the appropriate audio *.wav file and then click the **Open** button.
The selected file name is displayed in the *Install Music File* dialog box.

5 Optional. You can play the selected file by clicking the *Play* ( ) button.

a Click **Play Selected File** to play a file on your computer.

b Click **Play RMX File** to play a file already uploaded on the RMX.

6 In the *Install Music File* dialog box, click **OK** to upload the file to the MCU.
The new file replaces the previously uploaded file and this file is used for all background music played by the MCU.

Creating Audio Prompts and Video Slides

The RMX is shipped with default voice messages (in WAV format) and video slides that are used for the default IVR services. You can create your own video slides and record the voice messages for different languages or customize them to your needs.

Recording an Audio Message

To record audio messages, use any sound recording utility available in your computer or record them professionally in a recording studio. Make sure that recorded message can be saved as a Wave file (*.wav format) and that the recorded format settings are as defined in steps 4 and 5 on page 17-29. The files are converted into the RMX internal format during the upload process.
This section describes the use of the Sound Recorder utility delivered with Windows 95/98/2000/XP.

To define the format settings for audio messages:

- The format settings for audio messages need to be set only once. The settings will then be applied to any new audio messages recorded.
- The utility or facility used to record audio messages must be capable of producing audio files with the formats and attributes as shown in the following procedure, namely, **PCM**, **16.000kHz, 16Bit, Mono**.
  Windows® XP® Sound Recorder is one of the utilities that can be used.

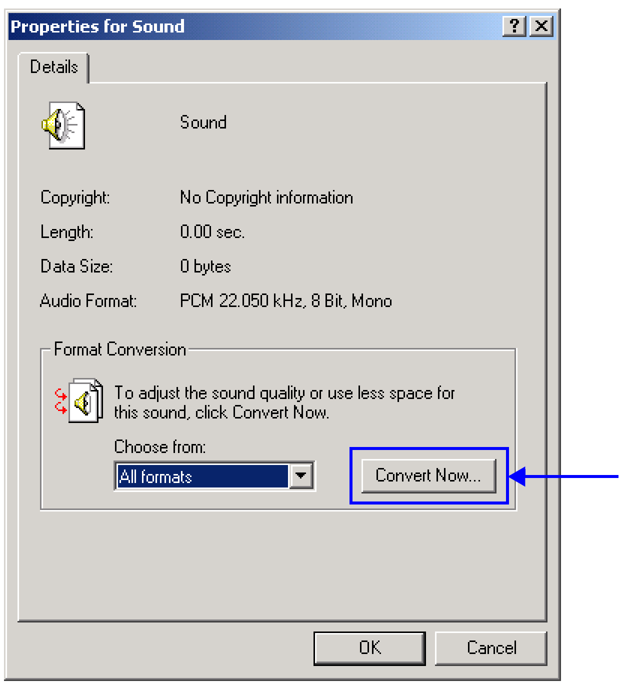
1 On your PC, click **Start** > **Programs** > **Accessories** > **Entertainment** > **Sound Recorder**.

The *Sound–Sound Recorder* dialog box opens.

2 To define the recording format, click **File** > **Properties**.

The *Properties for Sound* dialog box opens.

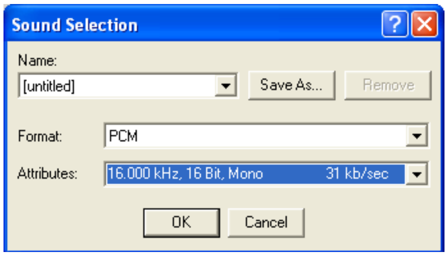
3 Click the **Convert Now** button.



The *Sound Selection* dialog box opens.

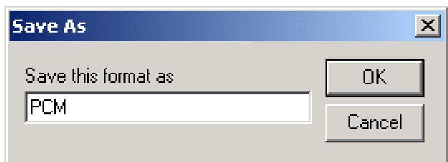
4 In the *Format* field, select **PCM**.

5 In the *Attributes* list, select **16.000 kHz, 16Bit, Mono.**



6 To save this format, click the **Save As** button.
The *Save As* dialog box opens.

7 Select the location where the format will reside, enter a name and then click **OK**.



The system returns to the *Sound Selection* dialog box.

8 Click **OK**.
The system returns to the *Properties for Sound* dialog box.

9 Click **OK**.
The system returns to the *Sound–Sound Recorder* dialog box. You are now ready to record your voice message.

To record a new audio message:

Regardless of the recording utility you are using, verify that any new audio message recorded adheres to the following format settings: **16.000kHz, 16Bit, Mono**.

Make sure that a microphone or a sound input device is connected to your PC.

1 On your PC, click **Start** > **Programs** > **Accessories** > **Entertainment** > **Sound Recorder**.

The *Sound–Sound Recorder* dialog box opens.

2 Click **File** > **New**.

3 Click the **Record** button.
The system starts recording.

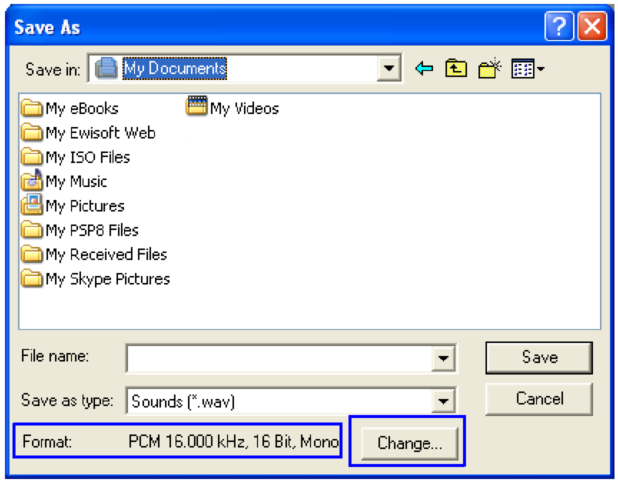
4 Start narrating the desired message.

For all audio IVR messages, stop the recording anytime up to 3 minutes (which is the maximum duration allowed for an IVR voice message). If the message exceeds 3 minutes it will be rejected by the RMX unit.

5 Click the **Stop Recording** button.

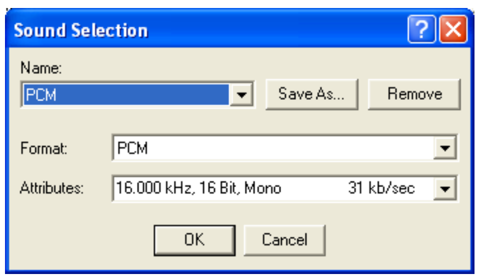
6 Save the recorded message as a wave file, click **File** > **Save As**.

The *Save As* dialog box opens.



7 Verify that the *Format* reads: **PCM 16.000 kHz, 16Bit, Mono**. If the format is correct, continue with step 10. If the format is incorrect, click the **Change** button.

The *Sound Selection* dialog box is displayed.



8 In the *Name* field, select the name of the format created in step 7 on page **17-30**.

9 Click **OK**.

The system returns to the *Save As* dialog box.

10 In the *Save in* field, select the directory where the file will be stored.

11 In the *Save as Type* field, select the ***.wav** file format.

12 In the *File name* box, type a name for the message file, and then click the **Save** button.

13 To record additional messages, repeat steps 1 to 10.

To upload your recorded *.wav file to the RMX, see step 6 on **page 17-8**.

Creating a Welcome Video Slide

The video slide is a still picture that can be created in any graphic application.

To create a welcome video slide:

1 Using any graphic application, save your image in either ***.jpg** or ***.bmp** file format.

2 For optimum quality, ensure that the image dimensions adhere to the RMX recommended values (width x height in pixels):

— 128 x 96
— 176 x 144
— 352 x 240
— 320 x 240
— 352 x 288
— 720 x 400
— 640 x 480
— 704 x 480
— 848 x 480
— 720 x 576
— 704 x 576
— 1024 x 576
— 960 x 720
— 1280 x 720
— 1440 x 1088
— 1920 x 1088

The RMX can accommodate small deviations from the recommended slide resolutions.

3 Save your file.

To upload your video slide to the RMX, see step 12 on **page** 17-25.

If using a default Polycom slide, the slide's resolution will be as defined in the profile, i.e. SD, HD or CIF.
If the display of the Welcome slide is cut in the upper area of the screen, change the settings of the endpoint's monitor to People "Stretch" instead of "Zoom".

Inviting Participants using DTMF

A participant in a video or audio conference can invite another participant to the conference using the touch-tone DTMF numeric keypad on the participant's endpoint. You can invite a participant using various communication devices, such as a mobile phone, an IP phone, PSTN phones, laptops, or connect to another conference running on another PBX or MCU.

Invite Call Flow

The following flow describes how a participant is invited to the conference using the DTMF codes:

1. During the conference, the participant enters the DTMF code (default is ***72**) on the numeric keypad to invite another participant.
2. The participant is prompted to enter the invited participant's destination number (a number or IP address) including the prefix (if required) and the DTMF delimiter digit ('*' or '#') at the end. The asterisk ('*') is used to denote the dot in the IP address.

   For example: To enter an IP address such as 10.245.22.19, on the DTMF keypad press 10*245*22*19 and then the DTMF delimiter.

> Digits that are entered after the DTMF delimiter and before the participant is connected are ignored.

3. The system automatically dials to the destination according to the protocol order as defined in the *IVR Services Properties - Video Services* tab.

   When the call cannot be completed by the current protocol, the system attempts to connect to the destination using the next protocol according to the protocol order.

   The RMX connects the participant when the call is answered.
4. The last invited participant can be disconnected when the inviting participant enters the DTMF code (default is **#72**) on the numeric keypad.

Entering Additional DTMF Codes

In some environments, the call is answered by an IVR system (for example when connecting to another conference or PBX), requesting a password or a destination number to complete the connection process. In such a case, additional DTMF digits must be entered before the **DTMF forward duration** time has expired and are forwarded to the invited destination. When the additional DTMF codes are entered, they are heard by all the conference participants.

If the DTMF code is not entered on time or if the wrong DTMF code is entered, the participant is prompted for a new input. After the defined number of retries have elapsed, the call is ended.

Error Handling

- If the destination endpoint is busy or the participant did not answer, the system ends the call.
- When an incorrect number is entered, the call fails and an error message is displayed.
- If the destination number is not entered in a specific amount of time (defined in **Timeout for user input** in the *IVR Services - Global* tab), the participant is prompted to enter a destination number again. Depending on the **Number of user input retries** as

defined in the *IVR Services - Global* tab, the system will attempt to receive the required input. When all the retries have failed, the call to the invited participant is cancelled.

Guidelines

- Participants can be invited to CP and VSW conferences.
- All network protocols are supported (H.323, SIP, ISDN, and PSTN). It is recommended to select PSTN and not ISDN if PSTN is the only destination protocol. If both PSTN and ISDN are enabled, it is recommended to select the PSTN before ISDN as the connection process for PSTN endpoints will be quicker.
- In an Multiple IP Networks environment, the system will try to connect the participant using each of the IP Network Services listed in the *Conference Profile - Network Services* dialog box. Network services that are excluded from this list are skipped during the dialing sequence.
- In CP conferences, the participant initiating the invitation to another participant is able to view the dialing information and connection status. During the dialing process, the dialing string is displayed as the participant name which is replaced by the site name when connected to the conference.
- By default, all participants (Everyone) are granted permission to invite a participant to join a conference. To change the permission to the Chairperson, modify the *Permission* column in the *IVR Service - DTMF Codes* tab.

Enabling the Invite Participants using DTMF Option

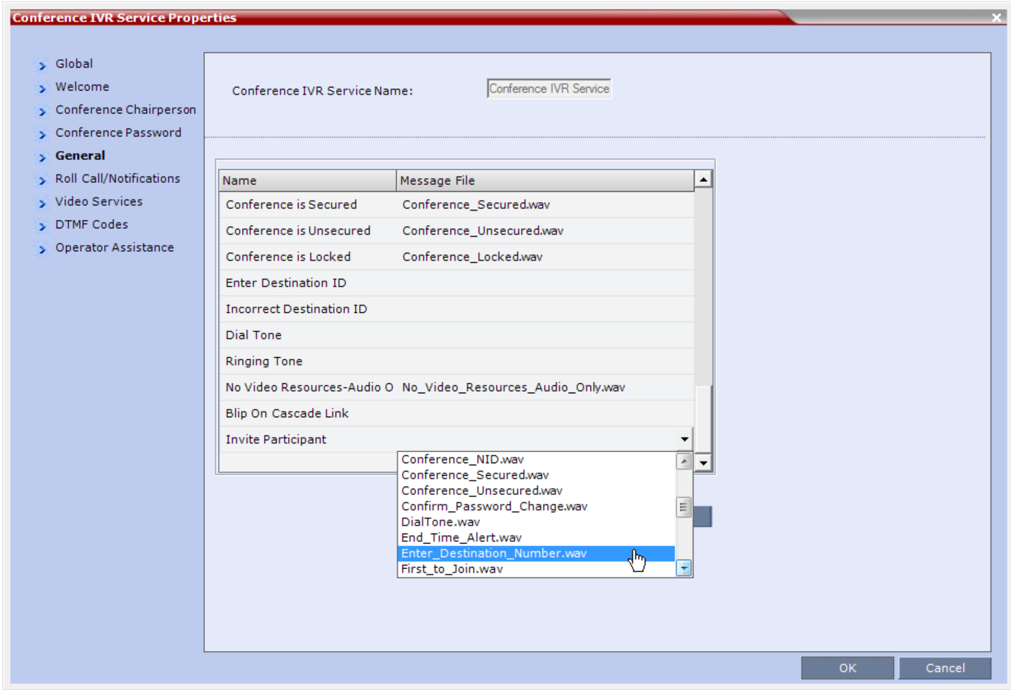
The option to invite participants to a conference using the DTMF keypad is enabled in the following *Conference IVR Services* dialog boxes:

- *General*
- *Video Services*
- *DTMF Codes*

To enable the Invite Participant using DTMF on the RMX:

1. Open an existing or define a new *Conference IVR Service*.
   Conference IVR Service - Global dialog box opens.
2. Click the **General** tab.

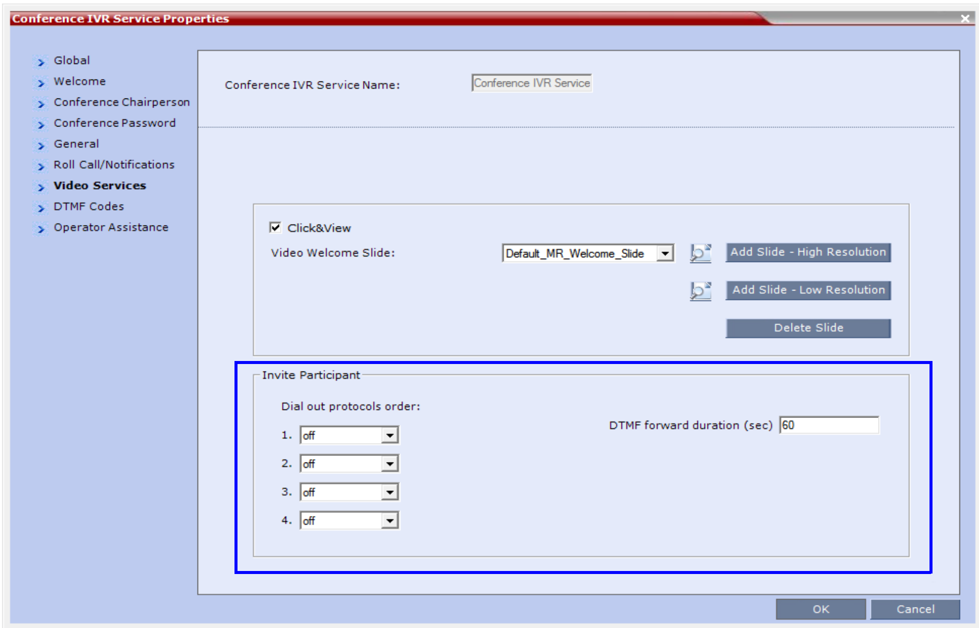
The *Conference IVR Services - General* tab is displayed.



3 In the Message File column of the **Invite Participant** entry, click the drop-down arrow and select the required voice message. The file **Enter_Destination_Number.wav** that is shipped with the system can be used for this message. To upload a new file, click the **Add Message File**. For more details, see "*Creating Audio Prompts and Video Slides"* on page 17-28.

4 Click the **Video Services** tab.

The *IVR Services - Video Services* tab is displayed.



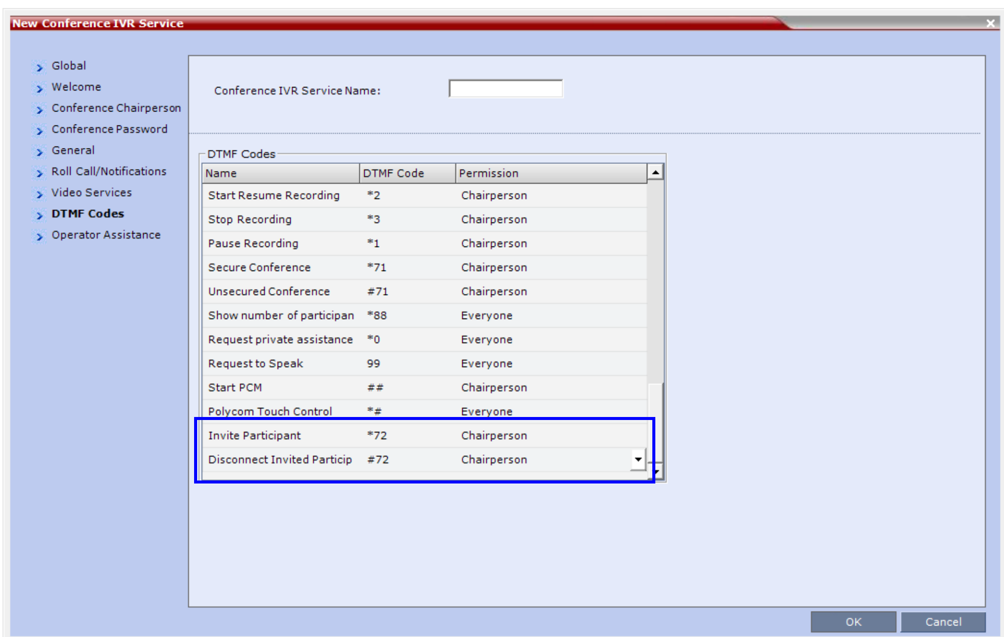
5 Define the following parameters:

Table 17-13 IVR Services Properties - Video Services Parameters - Invite Participants

Video Services	Description
Dial out protocols order	Select the order of the network protocols that will be used by the system to dial the destination number. The system will start dialing using the first protocol, and if the call is not answered it will continue with the second, third and fourth protocols (if they are enabled) until the call is answered. By default, H.323 is set as the first protocol and SIP as the second while the remaining protocols are disabled (set to Off). For PSTN calls, select the PSTN protocol and not ISDN. Set PSTN before ISDN if both PSTN and ISDN protocols are required.
DTMF forward duration	Use this field when connecting to another conferencing entity with an IVR, requiring the input of a password, destination number or ID. Enter the number of seconds that the system will wait for the input of additional DTMF digits such as a password or conference number. The range can be from 10 seconds to 600 seconds. Default is 60 seconds.

6 Click the **DTMF Codes** tab.

The I*VR Services - DTMF Codes* tab is displayed.



7 Make sure that **Invite Participant** and **Disconnect Invited Participant** have *DTMF Codes* assigned to them. Default system values are ***72** (*Invite Participant*) and **#72** (*Disconnect Invited Participant*), however you can enter your own values.
When upgrading from a previous version, default system values may not be assigned if these IVR entries were not defined in your existing IVR Service and have to be manually added to the *DTMF Codes* table.

8 If required, determine who can invite other participants to the conference using DTMF codes by changing the permissions to either **Chairperson** or **Everyone**.

9 Click **OK**.

Disabling the Invite Participant Option

To disable the Invite Participant option:

1 From the *IVR Services - DTMF Codes* tab, delete the DTMF digits from the **DTMF Code** column.

2 Click **OK**.

Default IVR Prompts and Messages

The system is shipped with the following audio prompts and messages:

Table 17-14 Default IVR Messages

Message Type	Message Text	File Name
General Welcome Message	"Welcome to unified conferencing."	General_Welcome.wav
Chairperson Identifier Request	"For conference Chairperson Services, Press the Pound Key. All other participants please wait..."	Chairperson_ Identifier.wav
Request Chairperson Password	"Please enter the Conference Chairperson Password. Press the pound key when complete."	Chairperson_Password.wav
Retry Chairperson Password	"Invalid chairperson password. Please try again."	Chairperson_ Password_Failure.wav
Request Password	"Please enter the conference password. Press the pound key when complete."	Conference_ Password.wav
Retry Password	"Invalid conference password. Please try again."	Retry_ Conference_ Password.wav
Request Digit	"Press any key to enter the conference."	Request_Digit.wav
Request Billing Code	"Please enter the Billing code. Press the pound key when complete."	Billing_Code.wav
Requires Chairperson	"Please wait for the chairperson to join the conference."	Requires Chairperson.wav
Chairperson Exit	"The chairperson has left the conference." **Note:** The *TERMINATE_CONF_AFTER_CHAIR_ DROPPED* flag must be enabled to play this message.	Chairperson_Exit.wav

Table 17-14 *Default IVR Messages (Continued)*

Message Type	Message Text	File Name
First to Join	"You are the first person to join the conference."	First to Join.wav
Mute All On	"All conference participants are now muted."	Mute_All_On.wav
Mute All Off	"All conference participants are now unmuted."	Mute_All_Off.wav
End Time Alert	"The conference is about to end."	End_Time_Alert.wav
Change Password Menu	"Press one to change conference password. Press two to change chairperson password. Press nine to exit the menu."	Change_Password_ Menu.wav
Change Conference Password	"Please enter the new conference password. Press the pound key when complete."	Change_ Conference_ Password.wav
Change Chairperson Password	"Please enter the new chairperson password. Press the pound key when complete."	*Change_ Chairperson_ Password.wav*
Confirm Password Change	"Please re-enter the new password. Press the pound key when complete."	*Confirm_ Password_ Change.wav*
Change Password Failure	"The new password is invalid."	*Change_ Password_ Failure.wav*
Password Changed Successfully	"The password has been successfully changed."	*Password_ Changed_ Successfully.wav*
Self Mute	"You are now muted."	*Self_Mute.wav*
Self Unmute	"You are no longer muted."	*Self_Unmute.wav*
Chairperson Help Menu	"The available touch-tone keypad actions are as follows: • To exit this menu press any key. • To request private assistance, press star, zero. • To request operator's assistance for the conference, press zero, zero. • To mute your line, press star, six. • To unmute your line, press pound, six."	*Chairperson_ Help_Menu.wav*

Table 17-14 *Default IVR Messages (Continued)*

Message Type	Message Text	File Name
Participant Help Menu	"The available touch-tone keypad actions are as follows: • To exit this menu press any key. • To request private assistance, press star, zero. • To mute your line, press star, six. • To unmute your line, press pound, six. • To increase your volume, press star, nine. • To decrease your volume, press pound, nine.	*Participant_Help_Menu.wav*
Maximum Participants Exceeded	"The conference is full. You cannot join at this time."	*Maximum_ Participants_ Exceeded.wav*
Roll Call Record	"After the tone, please state your name."	*Roll_Call_Record.wav*
Roll Call Joined	"...has joined the conference."	*Roll_Call _Joined.wav*
Roll Call Left	"...has left the conference."	*Roll_Call_Left.wav*
Roll Call Review	"The conference participants are..."	*Roll_Call_ Review.wav*
Request Conference NID	"Please enter your conference NID. Press the pound key when complete."	*Request_ Conference_NID.wav*
Retry Conference NID	"Invalid conference NID. Please try again."	*Retry_Conference_NID.wav*
Secured Conference	"The conference is now secured."	*Conference_Secured.wav*
Secured Conference	"The conference is now in an unsecured mode"	*Conference_Unsecured.wav*
Secured Conference	"Conference you are trying to join is locked"	*Conference_Locked.wav*
Conference Recording	"The conference is being recorded"	*Recording_ in_Progress.wav*
Conference Recording	"The conference recording has failed"	*Recording_Failed.wav*
No Video Resources Audio Only.	"All video resources are currently in use. Connecting using audio only"	*No_Video_Resources_Audio_ Only.wav*

Volume Control of IVR Messages, Music and Roll Call

The volume of IVR music, IVR messages and Roll Call is controlled by the following system flags:

- IVR_MUSIC_VOLUME
- IVR_MESSAGE_VOLUME
- IVR_ROLL_CALL_VOLUME

To control the volume of IVR music, messages and Roll Call:

>> Modify the values of the *System Flags* listed in Table 17-15 by clicking the menu **Setup > System Configuration**.

If these flags do not appear in the *System Flags* list, they must be manually added.

For more information see "*Modifying System Flags*" on page 22-1.

Table 17-15 *System Flags – IVR Volume Control*

Flag	Description
IVR_MUSIC_VOLUME	The volume of the IVR music played when a single participant is connected to the conference varies according to the value of this flag. Possible value range: 0-10 (Default: 5). 0 – disables playing the music 1 – lowest volume 10 – highest volume
IVR_MESSAGE_VOLUME	The volume of IVR messages varies according to the value of this flag. Possible value range: 0-10 (Default: 6). 0 – disables playing the IVR messages 1 – lowest volume 10 – highest volume **Note:** It is not recommended to disable IVR messages by setting the flag value to 0.
IVR_ROLL_CALL_VOLUME	The volume of the Roll Call varies according to the value of this flag. Possible value range: 0-10 (Default: 6). 0 – disables playing the Roll Call 1 – lowest volume 10 – highest volume **Note:** It is not recommended to disable the Roll Call by setting the flag value to 0.

The following *System Flags* do not require an MCU reset:

- IVR_MESSAGE_VOLUME
- IVR_MUSIC_VOLUME
- IVR_ROLL_CALL_VOLUME

For all other flag changes, the MCU must be reset for the modified flag settings (including deletion) to take effect.

18

The Call Detail Record (CDR) Utility

The Call Detail Record (CDR) utility enables you to view summary information about conferences, and retrieve full conference information and archive it to a file. The file can be used to produce reports or can be exported to external billing programs.

The value of the fields that support Unicode values, such as the info fields, will be stored in the CDR file in UTF8. The application that reads the CDR must support Unicode.

The Polycom RealPresence Collaboration Server (RMX) can store details of up to 2000 (RealPresence Collaboration Server (RMX) 1500/2000) or 4000 (RealPresence Collaboration Server (RMX) 4000) conferences. When this number is exceeded, the system overwrites conferences, starting with the earliest conference. To save the conferences' information, their data must be retrieved and archived. The frequency with which the archiving should be performed depends on the volume of conferences run by the MCU.

The RMX displays Active Alarms before overwriting the older files, enabling the users to backup the older files before they are deleted.

The display of Active Alarms is controlled by the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS System Flag.

If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file storage capacity limit, an Active Alarm is created: "Backup of CDR files is required".

Each conference is a separate record in the MCU memory. Each conference is archived as a separate file. Each conference CDR file contains general information about the conference, such as the conference name, ID, start time and duration, as well as information about events occurring during the conference, such as adding a new participant, disconnecting a participant or extending the length of the conference.

The CDR File

CDR File Formats

The conference CDR records can be retrieved and archived in the following two formats:

- **Unformatted data** – Unformatted CDR files contain multiple records in "raw data" format. The first record in each file contains general conference data. The remaining records contain event data, one record for each event. Each record contains field values separated by commas. This data can be transferred to an external program such as Microsoft Excel© for billing purposes.

The following is a sample of an unformatted CDR file:

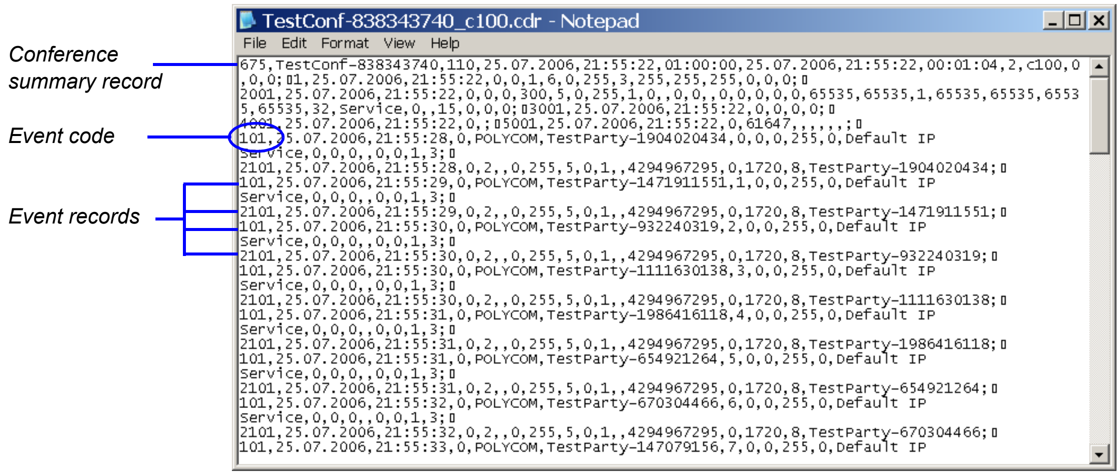


***Figure 18-1** Unformatted CDR File*

- **Formatted text** – Formatted CDR files contain multiple sections. The first section in each file contains general conference data. The remaining sections contain event data, one section for each event. Each field value is displayed in a separate line, together with its name. This data can be used to generate a summary report for a conference

> The field names and values in the formatted file will appear in the language being used for the *RealPresence Collaboration Server Web Client* user interface at the time when the CDR information is retrieved.

The following is an example of a formatted CDR file:

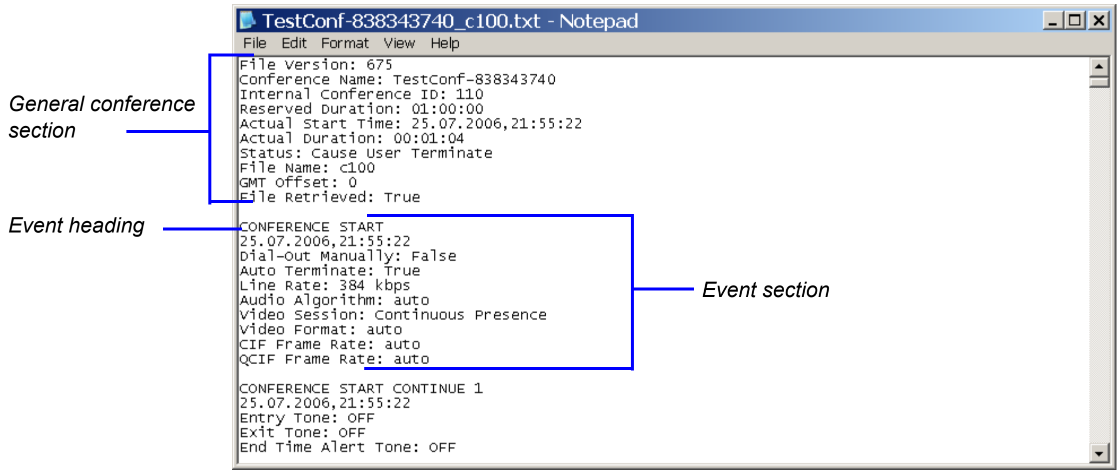


***Figure 18-2** Formatted CDR File*

Multi-Part CDR Files

By default, the maximum CDR (Call Data Record) file size is limited to 1MB. When a *CDR* file reaches a size of 1MB the file is saved and further call data recording is stopped and the additional data is lost.

The RMX can be configured to keep recording the data in multiple CDR file set of 1MB each. *Multi-Part CDR* ensures that conference call data from long duration or permanent conferences is recorded and not lost.

Guidelines

- *Multi-Part CDR* is enabled by setting the value of the **ENABLE_MULTI_PART_CDR** *System Flag* to **YES**.

  The flag's default value is **NO**.

  When the flag value is **NO,** *CDR* file size is limited to one file of 1MB and further call data recording is stopped.

  To modify the default setting, the flag must be manually added to the *System Configuration*. For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Modifying System Flags"* on page **22-1**.
- If the flag value is set to **YES**, when a *CDR* file reaches 1MB, an additional *CDR* file is created and added to the *CDR* file set for that conference.
- If the flag value is changed from **YES** to **NO** (or visa versa) all existing *CDR* files are retained.

CDR File Contents

The general conference section or record contains information such as the Routing Name and ID, and the conference starting date and time.

The event sections or records contain an event type heading or event type code, followed by event data. For example, an event type may be that a participant connects to the conference, and the event data will list the date and time the participant connects to the conference, the participant name and ID, and the participant capabilities used to connect to the conference.

To enable compatibility for applications that written for the MGC family, the RealPresence Collaboration Server CDR file structure is based on the MGC CDR file structure.

The unformatted and formatted text files contain basically the same information. The following differences should be noted between the contents of the unformatted and formatted text files:

- In many cases a formatted text file field contains a textual value, whereas the equivalent unformatted file field contains a numeric value that represents the textual value.
- For reading clarity, in a few instances, a single field in the unformatted file is converted to multiple fields in the formatted text file, and in other cases, multiple fields in the unformatted file are combined into one field in the formatted file.
- To enable compatibility between MGC CDR files and RealPresence Collaboration Server CDR files, the unformatted file contains fields that were applicable to the MGC MCUs, but are not supported by the RealPresence Collaboration Server MCUs. These fields are omitted from the formatted text file.

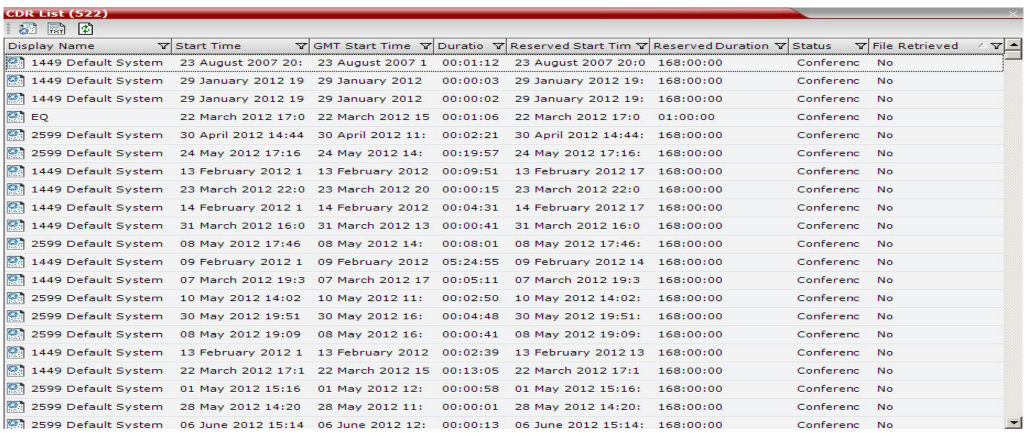
Appendix C: "*CDR Fields - Unformatted File”* on page **C-1**, contains a full list of the events, fields and values that appear in the unformatted file. This appendix can be referred to for information regarding the contents of fields in the unformatted text file, but does not reflect the exact contents of the formatted text file.

Viewing, Retrieving and Archiving Conference Information

Viewing the Conference Records

To open the CDR utility:

- On the *RMX Menu*, click **Administration > CDR**.
  The *CDR List* pane opens, displaying a list of the conference CDR records stored in the MCU memory.


CDR List (522)

Display Name	Start Time	GMT Start Time	Duratio	Reserved Start Tim	Reserved Duration	Status	File Retrieved
1449 Default System	23 August 2007 20:	23 August 2007 1	00:01:12	23 August 2007 20:0	168:00:00	Conferenc	No
1449 Default System	29 January 2012 19	29 January 2012	00:00:03	29 January 2012 19:	168:00:00	Conferenc	No
1449 Default System	29 January 2012 19	29 January 2012	00:00:02	29 January 2012 19:	168:00:00	Conferenc	No
EQ	22 March 2012 17:0	22 March 2012 15	00:01:06	22 March 2012 17:0	01:00:00	Conferenc	No
2599 Default System	30 April 2012 14:44	30 April 2012 11:	00:02:21	30 April 2012 14:44:	168:00:00	Conferenc	No
2599 Default System	24 May 2012 17:16	24 May 2012 14:	00:19:57	24 May 2012 17:16:	168:00:00	Conferenc	No
1449 Default System	13 February 2012 1	13 February 2012	00:09:51	13 February 2012 17	168:00:00	Conferenc	No
1449 Default System	23 March 2012 22:0	23 March 2012 20	00:00:15	23 March 2012 22:0	168:00:00	Conferenc	No
1449 Default System	14 February 2012 1	14 February 2012	00:04:31	14 February 2012 17	168:00:00	Conferenc	No
1449 Default System	31 March 2012 16:0	31 March 2012 13	00:00:41	31 March 2012 16:0	168:00:00	Conferenc	No
2599 Default System	08 May 2012 17:46	08 May 2012 14:	00:08:01	08 May 2012 17:46:	168:00:00	Conferenc	No
1449 Default System	09 February 2012 1	09 February 2012	05:24:55	09 February 2012 14	168:00:00	Conferenc	No
1449 Default System	07 March 2012 19:3	07 March 2012 17	00:05:11	07 March 2012 19:3	168:00:00	Conferenc	No
2599 Default System	10 May 2012 14:02	10 May 2012 11:	00:02:50	10 May 2012 14:02:	168:00:00	Conferenc	No
2599 Default System	30 May 2012 19:51	30 May 2012 16:	00:04:48	30 May 2012 19:51:	168:00:00	Conferenc	No
2599 Default System	08 May 2012 19:09	08 May 2012 16:	00:00:41	08 May 2012 19:09:	168:00:00	Conferenc	No
1449 Default System	13 February 2012 1	13 February 2012	00:02:39	13 February 2012 13	168:00:00	Conferenc	No
1449 Default System	22 March 2012 17:1	22 March 2012 15	00:13:05	22 March 2012 17:1	168:00:00	Conferenc	No
2599 Default System	01 May 2012 15:16	01 May 2012 12:	00:00:58	01 May 2012 15:16:	168:00:00	Conferenc	No
2599 Default System	28 May 2012 14:20	28 May 2012 11:	00:00:01	28 May 2012 14:20:	168:00:00	Conferenc	No
2599 Default System	06 June 2012 15:14	06 June 2012 12:	00:00:13	06 June 2012 15:14:	168:00:00	Conferenc	No

The following fields are displayed:

***Table 18-1** Conference Record Fields*

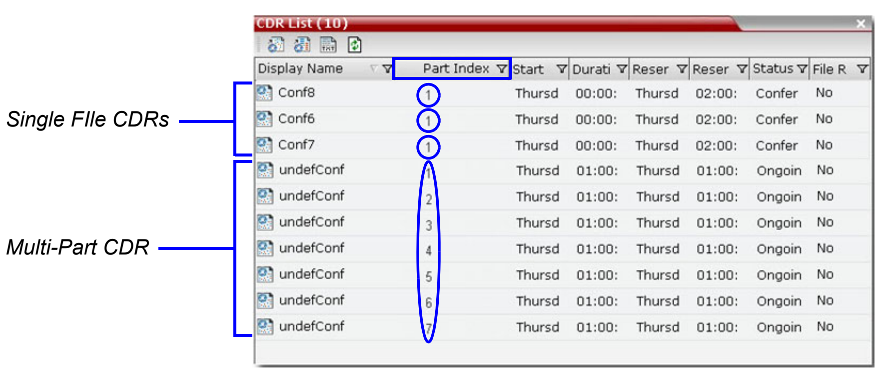
Field	Description
Display Name	The Display Name of the conference and an icon indicating whether or not the CDR record has been retrieved and saved to a formatted text file. The following icons are used:  The CDR record has not been saved.  The CDR record has been saved.
Start Time	The actual time the conference started.
GMT Start Time	The actual time the conference started according to Greenwich Mean Time (GMT).
Duration	The actual conference duration.

***Table 18-1** Conference Record Fields (Continued)*

Field	Description
Reserved Start Time	The reserved start time of the conference. If the conference started immediately this is the same as the *Start Time.*
Reserved Duration	The time the conference was scheduled to last. Discrepancy between the scheduled and the actual duration may indicate that the conference duration was prolonged or shortened.
Status	The conference status. The following values may be displayed: • ***Ongoing Conference*** • ***Terminated by User*** • ***Terminated when end time passed*** • ***Automatically terminated when conference was empty*** – The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. • ***Conference never became ongoing due to a problem*** • ***Unknown error*** **Note:** If the conference was terminated by an MCU reset, the status **Ongoing Conference** will be displayed.
File Retrieved	Indicates if the conference record was downloaded using any of the file retrieval buttons in the CDR List pane or the API. • **Yes** - when the conference record was retrieved to any file or using the API. • **No** - when the conference record was not retrieved at all. The File Retrieved field is updated whenever the record is downloaded.

Multi-part CDR File display

When the *Multi-Part CDR* is configured on the RMX, an additional column, *Part Index*, is added to the CDR list.



The *Part Index* column displays the *CDR* file's sequence in the CDR file set:

- *CDRs* that are up to 1MB consist of a single file. Each file has a unique *Display Name* and a *Part Index* of **1**.

- Files included in a *Multi-Part CDR* file sets have the same *Display Name*. The first file of the set is numbered **1** with each additional *CDR* file numbered in an ascending numeric sequence.

Refreshing the CDR List

To refresh the CDR list:

- Click the **Refresh** button, or right-click on any record and then select **Refresh**. Updated conference CDR records are retrieved from the MCU memory.

Retrieving and Archiving Conference CDR Records

To retrieve and archive CDR records:

1 To retrieve a single CDR record, right-click the record to retrieve and then select the required format (as detailed in Table 18-2).
Alternatively, select the record to retrieve, and then click the appropriate button on the toolbar (as detailed in Table 18-2).

To retrieve multiple CDR records simultaneously, use standard Windows multi-selection methods.

***Table 18-2** Conference Information Retrieval Options*

Menu Option	Button	Action
Retrieve		Retrieves the conference information as unformatted data into a file whose extension is .cdr.
Retrieve Formatted XML		Retrieves the conference information as formatted text into a file whose extension is .xml. Note: Viewed when logged in as a special support user.
Retrieve Formatted		Retrieves the conference information as formatted text into a file whose extension is .txt.

The *Retrieve* dialog box opens.
The dialog box displays the names of the destination CDR files.

2 Select the destination folder for the CDR files and then click **OK**.

If the destination file already exists, you will be asked if you want to overwrite the file or specify a new name for the destination file.
The files are saved to the selected folder.

CDR files are not included in the backup process and should be backed up manually by saving the CDR files to a destination device.

19

Gateway Calls

> Gateway calls are supported in AVC Conferencing Mode only.

The RealPresence Collaboration Server (RMX) can be used as a gateway that provides connectivity across different physical networks and translates multiple protocols for point-to-point rich media communications.

The RMX supports the widest range of video and audio algorithms. It allows sites with different frame rates, connection speeds, audio algorithms, video resolutions and network protocols to transparently connect with one another. It also enables multipoint conference creation from an endpoint.

A special conference acting as a *Gateway Session* is created on the RMX. It includes one dial-in connection of the endpoint initiating the *Gateway Session* and one or several dial-out connections to endpoints. It provides connectivity between the various protocols: H.323, SIP, ISDN and PSTN.

To enable the gateway functionality a special Gateway Profile is defined on the RMX.

Gateway Functionality

The following features and capabilities are supported in gateway calls:

- *Gateway Sessions* are in CP mode only.
  If Video Switching is selected in the *Profile* assigned to the *Gateway Session*, the system ignores this setting and will run the *Gateway Session* in CP mode.
  - From Version 7.2, *Gathering* phase is not supported in gateway calls, even if it is defined in the Profile assigned to the *Gateway Profil*e.
- H.239 Content
- FECC - IP participants only as FECC is not supported by the ISDN protocol.
- Recording. The *Recording Link* is not considered as a participant and therefore, the gateway session will automatically end when only one of the participants remains connected in addition to the recording link. The video of the *Recording Link* is not included in the display of the video of the gateway call.
- Forwarding of DTMF codes from the *Gateway Session* to a conference running on another gateway, MCU or DMA. This enables the participant to enter the required conference and/or chairperson password when connecting to another conference. DTMF forwarding is enabled when there are only two participants connected to the *Gateway Session*.
- Forwarding of all *DTMF* codes sent by participants in the *Gateway Session* to all *PSTN* and *ISDN* participants. This is enabled by adding the **ALWAYS_FORWARD_DTMF_IN_GW_SESSION_TO_ISDN** *System Flag* to *system.cfg* and setting its value to **YES**.

- Up to 80 gateway calls (same as conferences) may be run on a fully configured MCU.
- *Gateway Profiles* are included in the *Backup* and *Restore Configuration* operations.
- CDR files are generated for *Gateway Sessions* in the same way as for conferences.
- Cascading. To support cascading, the gateway indicates a lower number than the MCU for master-slave relation (directly or through DMA).
- Gateway calls are supported in Microsoft and Avaya environments.

Call Flows

Call flow changes according to the connection protocols: IP or ISDN. This section describes the call flows between two endpoints connect via one gateway. For call flows describing connections between two endpoints via two gateways, or a connection of an endpoint to a conference running on MCU via a gateway, see "*Basic Cascading using ISDN Cascaded Link"* on page **5-5**.

IP Participants

Two calling methods are available:

- **Direct** - the dialing string includes the destination number/conference ID and the call is routed directly to the destination endpoint/conference. This is the recommended method.
- **Via Gateway IVR** - the call connects to the gateway, where through interaction with the IVR, the destination number is entered using DTMF codes.

Direct Dialing

The calling endpoint enters the dialing string that includes the access numbers to the *RMX Gateway Profile* and the number of the destination endpoint. Up to 10 destination numbers can be entered in one string.

The call connects to the RMX *Gateway Profile* and a *Gateway Session* is created. The dial-in participant is automatically connected to it.

During the connection phase, the number being dialed is displayed on the screen of the calling endpoint.

If the call is not answered or it cannot be completed using one communication protocol, the system will try to connect the endpoint using the next communication protocol according to the selected protocols in the following order: H.323, SIP and ISDN. PSTN numbers are identified separately and are dialed immediately without trying other connections.

If the call is busy, the system will not try to connect the endpoint using another protocol.

If the call is not completed after trying all possible protocols, the system displays the number that was dialed on the calling endpoint's screen and the reason for not completing the call. For details, see "*Connection Indications"* on page **19-22**.

When the call is connected, a new *Gateway Session* is created and added to the ongoing *Conferences* list.

Dialing from H.323 Endpoints

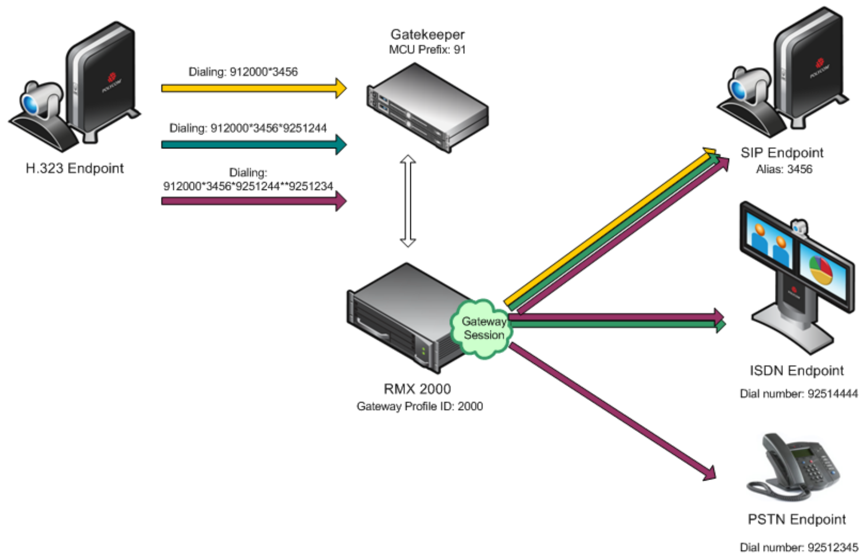


Figure 19-1*Dialing String and Call Flow from H.323 Endpoint to One, Two or Three Endpoints*

The calling endpoints can dial to one, two or several endpoints (up to ten) in one dialing string.

The dialing string includes the following components:

[MCU prefix in GK] - the prefix with which the RMX is registered to the gatekeeper.

[GW Profile ID] - The ID of the Gateway Profile to be used for routing the call to the destination endpoint or DMA, as defined in the *RMX Gateway Profiles*. It includes the parameters of the call to the destination.

***** - indicates H.323, SIP or ISDN connection protocol to the destination endpoint (followed by the appropriate destination number). Placing this delimiter before the destination number causes the system to try to connect the endpoint using H.323 first, then SIP and lastly ISDN according to the selected protocols.

****** - indicates a PSTN connection to the destination endpoint (followed by the appropriate destination number).

[Destination number] - the destination number as alias, IPv4 address or ISDN/PSTN number.

The dialing string:

[MCU prefix in GK][GW Profile ID]*[Destination Number, first participant]*[Destination Number, second participant][Destination number]......*[Destination Number, tenth participant]**

For example, If the *MCU Prefix in the GK* is 91 and the *GW Profile ID* is 2000, and the destination number is 3456 (SIP) enter: 912000*3456.

To invite two participants: SIP: 3456 and ISDN: 9251444, enter: 912000*3456*9251444.

To invite two participants: SIP: 3456 and a PSTN participant whose number is 9251234, enter: 912000*3456**9251234.

Dialing from SIP Endpoints

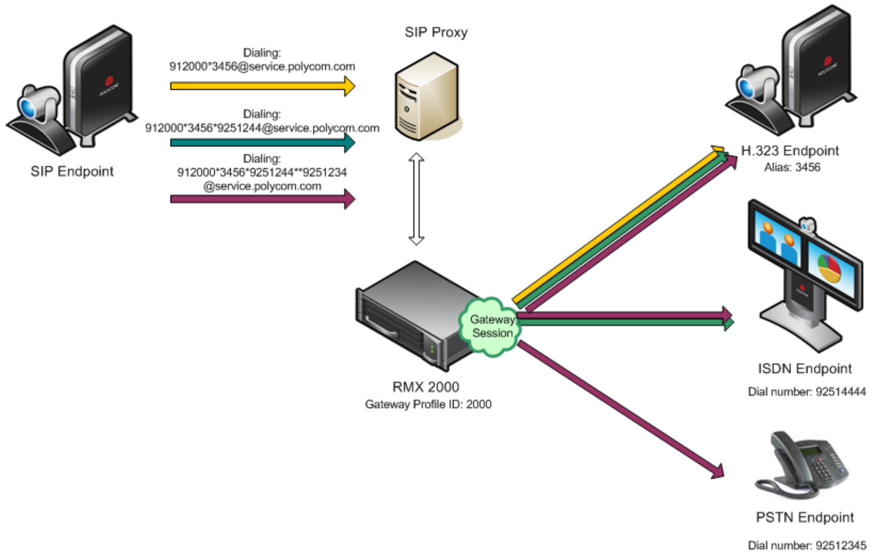


Figure 19-2*Dialing String and Call Flow from SIP Endpoint to One, Two or Three Endpoints*

The calling endpoints can dial to one, two or several endpoints (up to ten) in one dialing string. The dialing string includes the following components:

`[MCU Prefix in SIP Proxy]` - The prefix with which the RMX is registered to the SIP Proxy. This component is optional and is not required in most cases.

`[GW Profile ID]` - The ID of the Gateway Profile to be used for routing the call to the destination endpoint or DMA, as defined in the RMX Gateway Profiles. It includes the parameters of the call to the destination.

***** - indicates H.323, SIP or ISDN connection protocol to the destination endpoint (followed by the appropriate destination number). Placing this delimiter before the destination number causes the system to try to connect the endpoint using H.323 first, then SIP and lastly ISDN according to the selected protocols.

****** - indicates a PSTN connection to the destination endpoint (followed by the appropriate destination number).

`[Destination number]` - the destination number as alias, IPv4 address or ISDN/PSTN number.

`[@domain name]` - the RMX domain name as registered to the SIP Proxy

The dialing string:

`[GW Profile ID]*[Destination Number, first participant]*[Destination Number, second participant]**[destination number]......*[Destination Number, tenth participant]@domain name`

Optional:

```
[GW Profile ID]*[Destination Number, first participant]*[Destination
Number, second participant]**[destination
number]......*[Destination Number, tenth participant]@IP address of
the RMX signaling host
```

Optional:

```
[MCU prefix in SIP Proxy][GW Profile ID]*[Destination Number, first participant]*[Destination Number, second participant]**[destination number]......*[Destination Number, tenth participant]@domain name
```

For example, if the GW Profile ID is 2000, the domain name is service.polycom.com, and the destination number is 3456, enter: 2000*3456@service.polycom.com.

If using the IP address of the RMX signaling host (for example, 172.22.188.22) instead of the domain name enter: 2000*3456@172.22.188.22.

To invite two participants IP: 3456 and ISDN: 9251444, enter: 2000*3456*9251444@service.polycom.com.

To invite two participants IP: 3456 and PSTN: 9251234, enter: 912000*3456**9251234@service.polycom.com.

Gateway IVR

Can be used by IP endpoints when the destination dialing string includes the address of the MCU only. This is the same flow as the dialing method used for ISDN/PSTN calls, however it is less recommended for IP participants. For details, see page 19-8.

Dialing from H.323 Endpoints

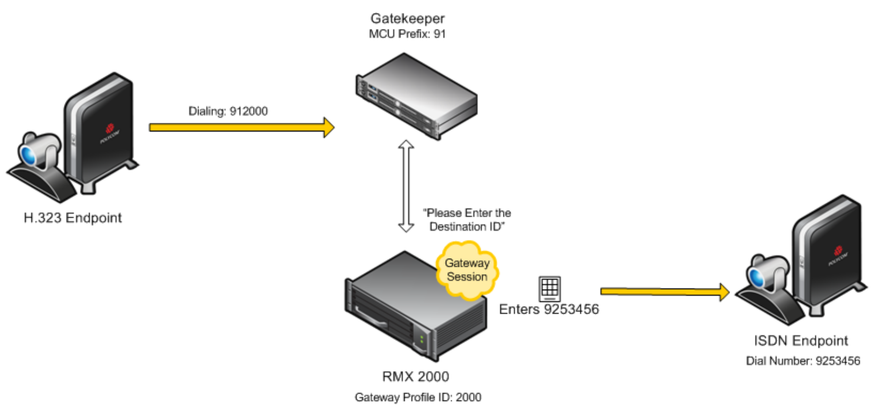


Figure 19-3Dialing String and Call Flow from IP Endpoint to ISDN Endpoint

`[MCU prefix in GK]` - the prefix with which the RMX is registered to the gatekeeper.

`[GW Profile ID]` - The ID of the Gateway Profile to be used for the gateway call and the IVR message.

The dialing string format is:

```
[MCU prefix in GK][GW Profile ID]
```

For example, if the MCU Prefix in the GK is 91 and the GW Profile ID is 2000 enter: 912000.

Once the participant is connected to the *Gateway Profile* and hears the IVR message requesting the destination number, using the DTMF input keypad, the participant enters the number of the destination endpoint followed by the # key. PSTN numbers are identified by an * before the number.

For example, enter 3456# for IP endpoint, or 9253456# for ISDN, or *9253456# for PSTN phone.

To enter an IP address as the destination number, replace the periods (.) with asterisks (*) in the format `n*n*n*n` followed by the # key. For example, if the IP address is 172.22.188.22, enter 172*22*188*22#.

Dialing from SIP Endpoints

Optional. `[MCU prefix in SIP Proxy]` - the prefix with which the RMX is registered to the gatekeeper.

`[GW Profile ID]` - The ID of the Gateway Profile to be used for the gateway call and the IVR message.

`[@domain name]` - the RMX domain name as registered to the SIP Proxy.

The dialing string:

`[GW Profile ID]@domain name`

Optional:

`[GW Profile ID]@IP address of the RMX signaling host`

Optional:

`[MCU prefix in SIP proxy][GW Profile ID]@domain name`

Once the participant is connected to the *Gateway Profile* and hears the IVR message requesting the destination number, using the DTMF input keypad, the participant enters the number of the destination endpoint followed by the # key. PSTN numbers are identified by an * before the number.

For example, enter 3456# for IP endpoint, or 9253456# for ISDN, or *9253456# for PSTN phone.

To enter an IP address as the destination number, replace the periods (.) with asterisks (*) in the format `n*n*n*n` followed by the # key. For example, if the IP address is 172.22.188.22, enter 172*22*188*22#.

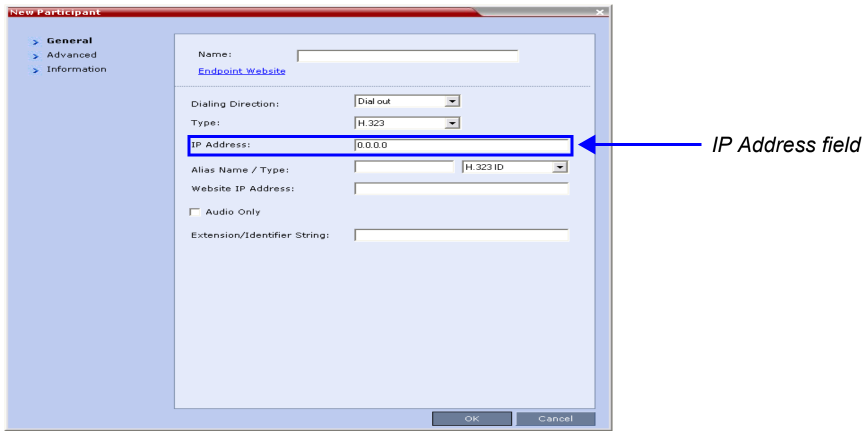
Direct IP Dialing

For RMXs registered to a gatekeeper, the *RMX* can be configured to dial and receive calls to and from *H.323* endpoints using the IP address in the event that the *Gatekeeper* is not functioning.

Dial-out Calls

For *Dial-out* calls, direct IP dialing is enabled or disabled by the **GK_MANDATORY_FOR_CALLS_OUT** *System Flag*.

When the flag is set to NO (default), if the *Gatekeeper* is not functioning, the RMX dials to the endpoint using the endpoint's IP address configured in the *IP Address* field of the *New Participant/ Participant Properties - General* dialog box.



If no IP address is defined in the *Participant Properties*, the call will fail.

The method by which calls are dialed out to the endpoint is dependant on the flag value and the availability of the *Gatekeeper* as summarized in the following table:

Table 19-1 *GK_MANDATORY_FOR_CALLS_OUT - System Flag*

Flag Value	Gatekeeper Available	Results
NO	NO	Dial out to endpoint *IP Address* **bypassing the Gatekeeper.**
NO	YES	Dial out to endpoint *Alias Name* using the *Gatekeeper.*
YES	NO	No dial out to endpoint.
YES	YES	Dial out to endpoint *Alias Name* using the *Gatekeeper.*

Dial-in Calls

For *Dial-in* calls, direct IP dialing is enabled or disabled by the **GK_MANDATORY_FOR_CALLS_IN** and *System Flag.*

When the flag is set to NO (default), if the *Gatekeeper* is not functioning, calls from endpoints will be connected directly to the *Entry Queue*, *Conference* or *Meeting Room* that was dialed.

The method by which dial-in calls are accepted or rejected is dependant on the flag value and the availability of the *Gatekeeper* as summarized in Table 19-2:

Table 19-2 *GK_MANDATORY_FOR_CALLS_IN - System Flag*

Flag Value	Gatekeeper Available	Results
NO	NO	Dial-in call is connected **bypassing the Gatekeeper.**
NO	YES	Dial-in call is connected using the *Gatekeeper.*
YES	NO	Dial-in call is rejected.

Table 19-2 GK_MANDATORY_FOR_CALLS_IN - System Flag (Continued)

Flag Value	Gatekeeper Available	Results
YES	YES	Dial-in call is connected using the *Gatekeeper.*

Enabling or Disabling Direct IP Dialing

The direct IP dialing is enabled by default. To disable it, manually add the flags **GK_MANDATORY_FOR_CALLS_OUT** and **GK_MANDATORY_FOR_CALLS_IN** to the *System Configuration - MCMS_PARAMETERS* dialog box and for each flag enter the required value (YES or NO).

For more information on flag definition, see "*Modifying System Flags*" on page **22-1**.

For flag changes (including deletion) to take effect, reset the RMX. For more information see "*Resetting the RMX*" on page **21-69**.

ISDN Participants

Two dialing methods are available to ISDN/PSTN participants:

- Via Gateway IVR
- Direct with automatically generated destination dial strings from dial-in strings. This dialing method is available from Version 7.1 and is supported on RMX with MPM+ and MPMx cards.

In addition, PSTN participants can dial the Gateway IVR and can use the MCU or DMA prefix in the gatekeeper together with the conference ID/endpoint alias as the destination string to simplify the input. This is one of the methods for PSTN participants to connect to a virtual Meeting Room on the DMA.

Gateway IVR

In this flow, the calling endpoint enters the dialing string that includes the access number to the *RMX Gateway Profile*.

The endpoint connects to the RMX and is welcomed by the IVR Welcome slide and message: "Please enter the destination number" followed by the dial tone.

Using the endpoint's DTMF input device such as remote control, the participant enters the number of the destination endpoint followed by the # key. Only one number can be dialed.

While the system dials to the destination endpoints, the participant hears the dialing rings. During the connection phase, the number being dialed is displayed on the screen of the calling endpoint.

If the call is not answered or it cannot be completed using one communication protocol, the system will try to connect the endpoint using the next communication protocol according to the selected protocols in the following order: H.323, SIP and ISDN.

PSTN numbers are identified separately and are dialed immediately without trying other connections.

If the endpoint is busy, the system will not try to connect the endpoint using another protocol.

If the call is not completed after trying all possible protocols, the system displays the number that was dialed on the calling endpoint's screen and the reason for not completing the call. For details, see "*Connection Indications"* on page **19-22**.

Dialing from ISDN/PSTN Endpoints

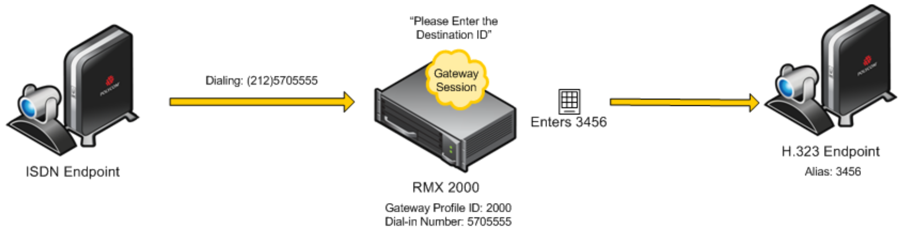


Figure 19-4*Dialing String and Call Flow from ISDN Endpoint to IP Endpoint*

`[GW Profile ISDN/PSTN number]` - the dial-in number assigned to the Gateway Profile, including the required country and area codes.

For example, if the dial-in number assigned to the Gateway Profile is 5705555, enter this number with the appropriate area code: 2125705555.

Once the participant is connected to the *Gateway Profile* and hears the IVR message requesting the destination number, using the DTMF input keypad, the participant enters the number of the destination endpoint followed by the # key. For example, enter 3456# for IP endpoint.

To enter an IP address as the destination number, replace the periods (.) with asterisks (*) in the format `n*n*n*n` followed by the # key. For example, if the IP address is 172.22.188.22, enter 172*22*188*22#.

PSTN Dial-in Using GK Prefix

When connecting to an RMX that is standalone or part of a *DMA* solution deployment, *PSTN* participants are prompted by an *IVR* message requesting the *Destination Conference ID* followed by the # key to be entered using the *DTMF* input keypad.

Including the *Gatekeeper Prefix* in the *DTMF* input string enables *PSTN* participants to use the input string when connecting to an RMX whether the RMX is a standalone *MCU* or part of a *DMA* solution deployment. For a detailed description, see "*PSTN Dial-in Using GK Prefix"* on page **19-9**.

Direct Dial-in to Endpoints or DMA VMR using Automatically Generated Destination Numbers

ISDN/PSTN participants can call the destination endpoints without interaction with the IVR of the gateway. This dialing method is enabled when the administrator configures the *Gateway Profile* to automatically generate the dial string of the destination endpoint or Meeting Room on the DMA by truncating the dial in string and replacing the truncated digits by other digits that can be used as the destination number.

For a detailed description of the call flow when dialing the DMA using this method, *see "Calling a DMA Direct with Automatically Generated Destination Dial Strings" on page* **19-26**.

Calling an IP Endpoint via Gateway

If the call destination is an IP endpoint, the endpoints must be registered to the same gatekeeper to which the RMX is registered. There should be a mapping between the dial-in numbers in the range defined for the ISDN Network Service and also assigned to the Gateway Profile and the IP endpoints, in such a way that the alias of each endpoint is the number that will be appended to the ISDN prefix.

When the call arrives to the gateway, this prefix is truncated and replaced by digits that correspond to the MCU prefix in the gatekeeper and the call is forwarded to the destination endpoint.

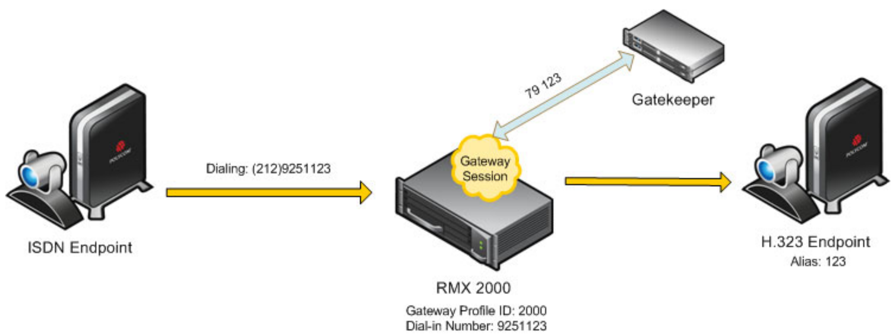


Figure 20 Call Flow from ISDN Endpoint to H.323 Endpoint with Automatically Generated Forwarded Dial String

For example:

- The ISDN prefix is 9251.
- The dial in number range defined in the ISDN Network Service can be 100 to 400 (that is, 9251100 to 9251400).
- The dial in numbers assigned to the Gateway Profile can the entire range, or part of the range of other Gateway Profiles are to be used: 100 to 200 (that is 9251100 to 9251200).
- The aliases assigned to the IP endpoints will range between 100 to 200 or 400 (for the full range) as well.
- MCU Prefix in the gatekeeper: 79.
- Number of digits to append (same as the ISDN prefix is this example): 3.
- The destination endpoint alias is 123.
- The ISDN endpoint dials 9251123. The RMX truncates the four first digits 9251 replacing them with 79 and appends 123 to 79, to create the destination number 79123 which is sent to the gatekeeper for routing.

Interoperability with CMA

The RMX does not register to the gatekeeper as a Gateway, therefore it is recommended to create and use the CMA *Dialing Rules* to enable the CMA Dial One Method.

When the caller enters the Dial One digit as the destination number prefix, the CMA replaces this digit with the MCU prefix in the Gatekeeper and the ID of the Gateway Profile. For example, the calling participant can enter 99251444, where 9 is the digit that is used as the MCU prefix registered in gatekeeper and is replaced by the gatekeeper with * and the Gateway Profile ID (for example, *2000) as defined in the Dialing Rule.

For more details on Dialing Rules definition in the CMA, see the *Polycom CMA System Operations Guide, "Dial Rule Operations"*.

Gateway Redial or Redialing Gateway Calls

Additional *Redial* options and *IVR* messages have been included for *Gateway Calls* to numbers that are wrong, adding functionality to the *RMX's Gateway* capabilities when used in conjunction with communication servers (*H.323, SIP, ISDN)* such as *Polycom's CMA* and *DMA*.

Guidelines

- *Redial* with *IVR* is supported:
  - With both *MPMx* and *MPM+* cards.
  - In *CP* environments only.
  - For *H.323, SIP* and *ISDN* calls.
  - When using the *RMX's Inviting Participants using DTMF* functionality.
- *Redial* with *IVR* is not supported:
  - When using *PCM's Invite Participant* functionality.
  - Dialing multiple destination numbers.

Redial on Wrong Number

In previous versions, calls to wrong numbers were disconnected, with no redial attempts or IVR messages.

In this version, an *IVR* message is played requesting the user to enter a new number, followed by up to five redial attempts. If all redial attempts fail, the user is alerted by an *IVR* message that the dialed number is unreachable, followed by reorder tone and disconnection.

Wrong Destination Number

- The number of re-dial attempts is controlled by the **WRONG_NUMBER_DIAL_RETRIES** *System Flag.*

  The default number of redial attempts is **3**. To modify the number of redial attempts, manually add the flag to *system.cfg* and set its value to the number of redial attempts required.

  The flag value range is **0-5**. A flag value of **0** means that no redials are attempted. For more information about *System Flags*, see "*Manually Adding and Deleting System Flags"* on page **22-18**.
- Redial attempts follow the same order as defined in the *Gateway Profile*: *H.323,* followed by *SIP,* followed by *ISDN*. For more information about *Gateway Profiles* and *Gateway Dial out Protocols*, see "*Defining the Gateway Profile"* on page **19-18**.
- *Redial on Wrong Number* is activated if a *Gateway Call* fails, for all defined protocols, for any reason or combination of reasons listed in Table 19-3.

Table 19-3 *Call Failure Reasons - H.323, SIP, ISDN*

H.323	SIP	ISDN
Unreachable Destination	484 - Address Incomplete	3 - No Route to Destination

Table 19-3 Call Failure Reasons - H.323, SIP, ISDN (Continued)

H.323	SIP	ISDN
Bad Format Address	404 - Not Found	18 - No User Responding
Adaptive Busy	414 - Request-URI Too Long	28 - Invalid Number Format
Admission Rejected (ARJ) Reason: Request Denied Item 1: Cannot find location.	416 - Unsupported URI Scheme	41 - Temporary Failure
Admission Rejected (ARJ) Reason: Called Party Not Registered	420 - Bad Extension	
	421 - Extension Required	

The user receives the *Redial on Wrong Number IVR* message: "*Incorrect destination. Please enter the destination number*".

If all the redial attempts fail the user receives the *Disconnect on Wrong Number IVR* message: "*Destination could not be reached; call is disconnected*".

- *Gateway Re-dial* is not activated if the reason for call failure is *Busy* or *No Answer*, for any of the defined protocols.

Wrong Destination Number Time-out

- A *time-out* counter is started when the *Redial on Wrong Number* message is played. If the user does not enter another destination number within the time-out period it is considered a failed dial out attempt.
- The *Redial on Wrong Number* message and *time-out* are repeated according to the value of the **WRONG_NUMBER_DIAL_RETRIES** *System Flag*. If there is no input from the user, after completing the retries, the user receives the *Disconnect on Wrong Number IVR* message: "*Incorrect destination number*" followed by the *Reorder Tone.*

Disconnect on Busy

As in previous versions, redialing of calls to busy destination numbers can be selected. The number of redial attempts is dependent on the **NUMBER_OF_REDIAL** *System Flag*, the default value is **3**. For more information see "*Defining New Profiles*" on page **2-18**.

In previous versions, if all retry attempts failed, there were no further call attempts with no notification.

When using this version, if all retry attempts fail, the user receives the *Disconnect on Busy* message in the form of *Busy Tone*. The call is then disconnected.

Disconnect on No Answer

In previous versions, if a call failed due to no answer at the destination, the call was disconnected with no notification.

When using this version, if all retry attempts fail, the user receives the *Disconnect on No Answer* message in the form of *Reorder Tone*. The call is then disconnected.

Disconnect on Wrong Number

In previous versions, if a call failed due to no answer at the destination, the call was disconnected with no notification.

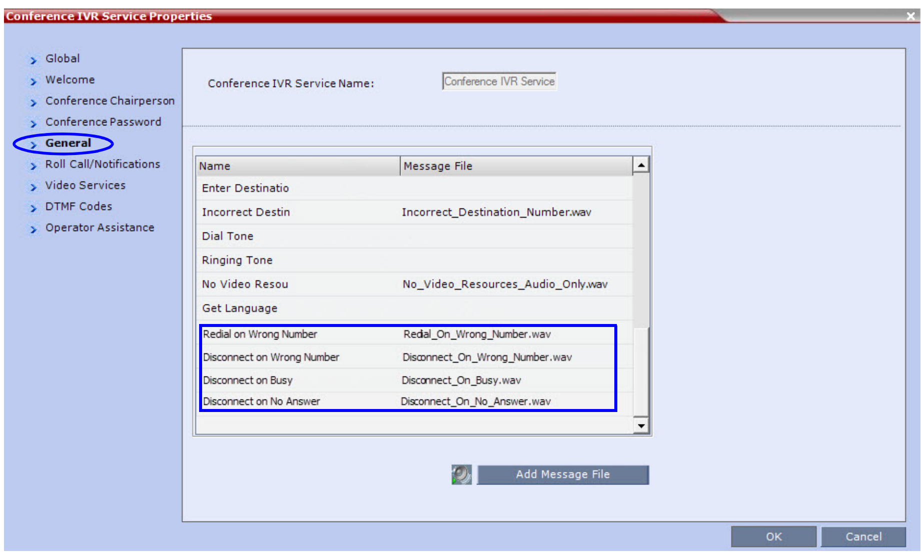
When using this version, the user receives the *Disconnect on Wrong Number IVR* message: *"Incorrect Destination Number"* followed by *Reorder Tone*. The call is then disconnected.

New IVR Messages

There are 4 new *IVR Messages*:

- *Redial on Wrong Number*
- *Disconnect on Wrong Number*
- *Disconnect on Busy*
- *Disconnect on No Answer*

IVR Messages are assigned and modified in the *General* tab of the *Conference IVR Service* or *Conference IVR Properties* dialog box.



For more information see "*IVR Services"* on page **17-1**.

Configuring the Gateway Components on the RMX

To enable gateway calls in the RMX, the following components have to be configured:

- *Conference IVR Service* to be used with the *Conference Profile* assigned to the *Gateway Profile*. The IVR Services are used for *Gateway IVR* connections.
- *Conference Profile* that includes the IVR Service for the Gateway Session and the settings to automatically terminate the Gateway Session when one participant is still connected or when no participants are connected
- *Gateway Profile* for call routing.

Defining the IVR Service for Gateway Calls

The system is shipped with a default Conference IVR Services for gateway calls named GW IVR Service that enables you to run gateway calls without defining a new Conference IVR Service. This IVR Service includes the following settings:

- *Welcome slide and message* - disabled
- *Conference and Chairperson Passwords* - disabled
- *General Messages* - all messages including the gateway messages and dial tones are selected
- *Roll Call* - disabled
- *Video Services - Click&View* - enabled
- *Video Services - Video Welcome Slide* - **Default_GW_Welcom_Slide**
- *Operator Assistance* - disabled

You can define a new Conference IVR Service to be used for gateway calls. This Conference IVR Service will be assigned to the appropriate Gateway Profile.

To define a new Conference IVR Service for gateway calls:

1 In the *RMX Management* pane, expand the *Rarely Used* list and click the **IVR Services** ( ) entry.
The list pane displays the *Conference IVR Services* list.

2 On the *IVR Services* toolbar, click the **New Conference IVR Service** ( ) button.
The *New Conference IVR Service - Global* dialog box opens.

3 In the *Conference IVR Service Name* field, enter a name that will identify this service as a gateway IVR service.

4 Define the IVR Service Global parameters (it is recommended to use the system defaults). For more details, see *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide*, "*Conference IVR Service Properties - Global Parameters*" on page 17-7.

5 When defining a gateway IVR Service, the following options should remain disabled:

— Welcome Messages (in the *Conference IVR Service - Welcome* dialog box).

— Chairperson Messages (in the *Conference IVR Service - Conference Chairperson* dialog box).

— Password Messages (in the *Conference IVR Service - Conference Password* dialog box)

6 Click the **General** tab.

The *General* dialog box lists messages that are played during the conference. These messages are played when participants or the conference chairperson perform various operations or when a change occurs.

7 To assign the appropriate audio file to the message type, click the appropriate table entry, in the *Message File* column. A drop-down list is enabled.

> For gateway redial, ensure that the audio files for the gateway redial messages have been assigned.

8 From the list, select the audio file to be assigned to the event/indication.

9 Repeat steps 7 and 8 to select the audio files for the required messages.

10 For a gateway IVR Service, select the audio file for the following message types:

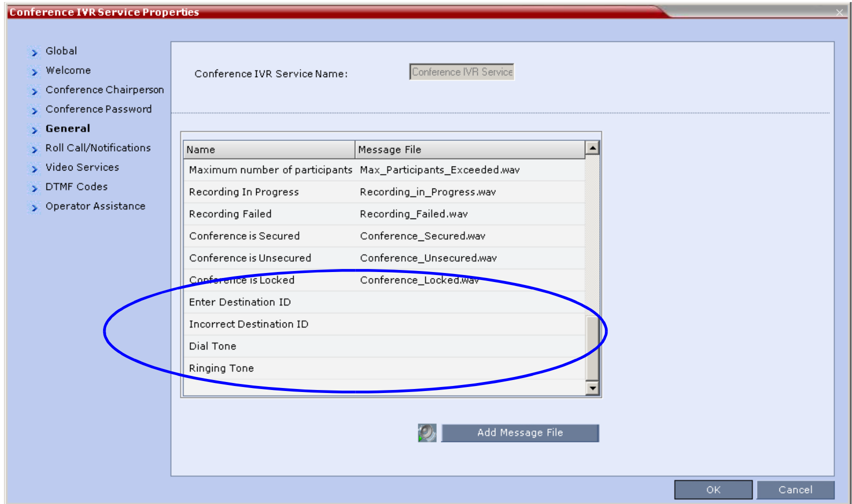


Table 19-4 *Conference IVR Service Properties - Gateway General Voice Messages*

Message Type	Description
Enter Destination ID	Prompts the calling participant for the destination number. Default message prompts the participant for the conference ID (same message as in the Entry Queue IVR Service).
Incorrect Destination ID	If the participant entered an incorrect conference ID (in gateway calls it is the destination number), requests the participant to enter the number again.
Dial Tone	The tone that will be played to indicate a dialing tone, to let the calling participant enter the destination number.
Ringing Tone	The tone that will be played to indicate that the system is calling the destination number.

11 When defining a gateway IVR Service, it is recommended that the *Roll Call* option remains disabled.

12 Click the **Video Services** tab.

The *New Conference IVR Service - Video Services* dialog box opens.

13 Define the following parameters:

Table 19-5 *New Conference IVR Service Properties - Video Services Parameters*

Video Services	Description
Click&View	Select this option to enable endpoints to run the Click&View application that enables participants to select a video layout from their endpoint.

Table 19-5 *New Conference IVR Service Properties - Video Services Parameters (Continued)*

Video Services	Description
Video Welcome Slide	Select the video slide file to be displayed when participants connect to the conference. To view any slide, click the **Preview Slide** ( ) button. If the video slide file was not uploaded to the MCU prior to the IVR Service definition, click the **Add Slide** button. The *Install File* dialog box opens. The uploading process is similar to the uploading of audio files. For more information, see step 7 on page **19-14**. **Notes:** • When using one of the default Polycom slides, the slide will be displayed in the resolution defined in the profile, i.e. CIF, SD, HD 720p or HD 1080p. • When defining a gateway IVR Service, the recommended default slide is: Default_GW_Welcome_Slide.

14 Click the **DTMF Codes** tab.
The *New Conference IVR Service - DTMF Codes* dialog box opens.

15 If required, modify the DTMF codes or permissions. For more details see "*New Conference IVR Service Properties - DTMF Codes"* on page **17-19**.

16 Click the **Operator Assistance** tab.

17 If Operator Assistance will not be available to participants, clear the **Enable Operator Assistance** option, which is automatically selected to disable it.

18 Click **OK** to complete the IVR Service definition.
The new Conference IVR Service is added to the *IVR Services* list.

Defining the Conference Profile for Gateway Calls

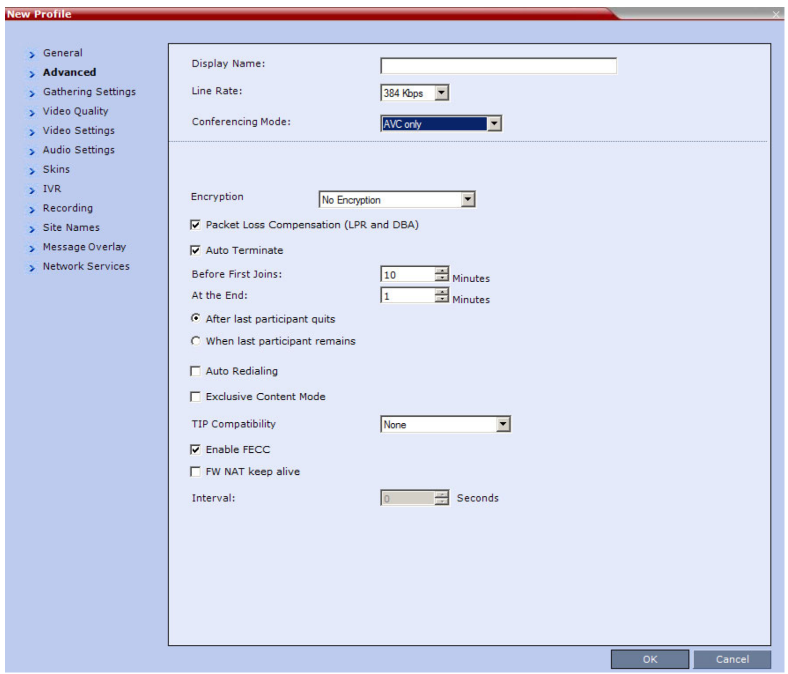
The Conference Profile that will be later assigned to the Gateway Profile determine the parameters of the gateway call, such as the line rate and video resolution and if to automatically terminate the gateway session when one participant or no participants are connected to the *Gateway Session*.

From Version 7.2, Gathering phase is not supported in gateway calls, even if it is defined in the Profile assigned to the Gateway Profile.

To define a Conference Profile for Gateway Sessions:

1. In the *RMX Management* pane, click **Conference Profiles**.
2. In the *Conference Profiles* pane, click the **New Profile** button.
   The *New Profile – General* dialog box opens.
3. Define the Profile name and select the line rate for the gateway session.
4. Click the **Advanced** tab.

   The *New Profile – Advanced* dialog box opens.



5. Define the required settings for *Encryption* and *LPR*.
6. Set the *Auto Terminate - At the End* option to **When Last Participant Remains** ensuring that the gateway call will end when only one participant is connected. For more details, see Table 2-9, “*New AVC Profile - Advanced Parameters,*” on page 2-22.
7. Define the remaining Profile parameters as described in "*Defining New Profiles”* on page 2-18.

Defining the Gateway Profile

A Gateway Profile is a conferencing entity, based on the Conference Profile assigned to it, that enables endpoints to dial-in and initiate *Gateway Sessions*. The system is shipped with a default Gateway Profile, named *Default_GW_Session*.

When an endpoint calls the Gateway Profile, a new *Gateway Session* is automatically created based on the Profile parameters, and the endpoint joins the gateway call which can also be a multipoint conference if more than two participants are connected to the conference.

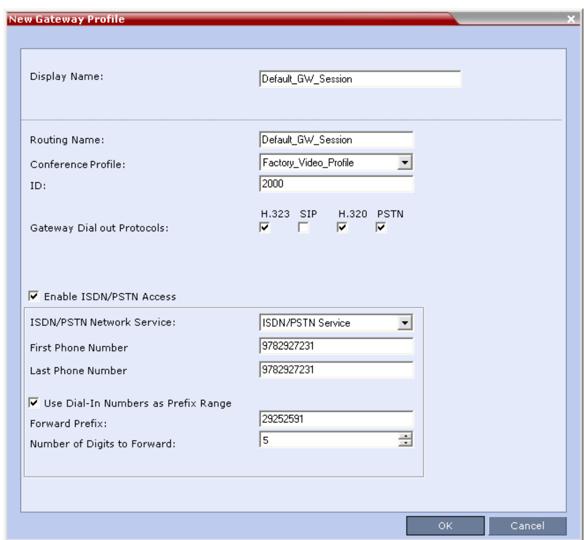
The *Gateway Profile* defines the parameters of the gateway call that are taken from the Conference Profile assigned to it, such as line rate, resolution, the IVR Service to be used and the dial-in numbers.

> Up to 1000 Gateway Profiles, Entry Queues, IP Factories and Meeting Rooms can be defined in the RMX (they are all part of one repository whose size is 1000 entries).

To define a new Gateway Profile:

1. In the *RMX Management - Rarely Used* pane, click **Gateway Profiles** .
2. In the *Gateway Profiles* list pane, click the **New Gateway Profile** button.

   The *New Gateway Profile* dialog box opens.



> Do not enable PSTN/ISDN access without defining the dial-in numbers range and/or the use of "Dial-In Numbers as Prefix Range". If you enable the PSTN/ISDN access without the definition of the dialing parameters, people can dial in to the gateway from outside the organization and then make long distance calls at the 'host' expense.

3 Define the following parameters:

Table 19-6 *New Gateway Profile Properties*

Option	Description
Display Name	Enter a unique-per-MCU name for the *Gateway Profile* in native language character sets to be displayed in the RealPresence Collaboration Server Web Client. The system automatically generates an ASCII name for the *Display Name* field that can be modified using Unicode encoding. • English text uses ASCII encoding and can contain the most characters (Maximum length in ASCII is 80 characters). • European and Latin text length is approximately half the length of the maximum. • Asian text length is approximately one third of the length of the maximum. The maximum length also varies according to the mixture of Unicode and ASCII.
Routing Name	The *Routing Name* is defined by the user, however if no *Routing Name* is entered, the system will automatically assign a new name when the Profile is saved as follows: • If an all ASCII text is entered in *Display Name*, it is used also as the *Routing Name.* • If any combination of Unicode and ASCII text (or full Unicode text) is entered in *Display Name*, the *ID* (such as Conference ID) is used as the *Routing Name.*
Conference Profile	The default Conference Profile is selected by default. If required, select the appropriate Profile from the list of Profiles defined in the MCU. **Note:** In the *Conference Profile - Advance* dialog box, the **Auto Terminate** option enables you to automatically terminate the *Gateway Session* when one participant remains connected (excluding the Recording Link). A new *Gateway Session* is created using the parameters defined in the Profile.
ID	Enter a unique number identifying this conferencing entity for dial in. Default string length is 4 digits. If you do not manually assign the ID, the MCU assigns one after the completion of the definition. The ID String Length is defined by the flag NUMERIC_CONF_ID_LEN in the System Configuration.
Gateway Dial out Protocols	Select the communication protocols to be used for dialing out to the destination participant(s). The system starts by connecting the participant using the first selected protocol. If the call is not answered or it cannot be completed using one communication protocol, the system will try to connect the endpoint using the next communication protocol in the following order: H.323, SIP and ISDN. PSTN numbers are identified separately and are dialed right away without trying other connections. By default, all protocols (H.323, SIP, ISDN and PSTN) are selected. Clear the protocol that should not be used for connecting the destination endpoint.

Table 19-6 *New Gateway Profile Properties (Continued)*

Option	Description
IP Network Service	Select the IP Network Service to be used with this Gateway. If this is not selected the default IP Network Service will be used.
Enable ISDN/PSTN Access	Select this check box to allocate dial-in numbers for ISDN/PSTN connections. To define the first dial-in number using the default ISDN/PSTN Network Service, leave the default selection. When the Entry Queue is saved on the MCU, the dial-in number will be automatically assigned to the Entry Queue. This number is taken from the dial-in numbers range in the default ISDN/PSTN Network Service. **Note:** Even if ISDN/PSTN is disabled for dial-in, if an ISDN/PSTN Network Service is defined in the system, and ISDN and/or PSTN are enabled for dialed out, the system will used the default ISDN Network Service for dialing out to the target number.
ISDN/PSTN Network Service	The default Network Service is automatically selected. To select a different ISDN/PSTN Network Service in the service list, select the name of the Network Service. **Note:** If you enable the ISDN/PSTN access, define the dial-in phone number ranges and the *Use Dial-In Numbers as Prefix Range parameters* to prevent abuse of the *gateway.*
First Phone Number	Enter the first number in the *Dial-in* number range to be used for dialing into the gateway. This number must be part of the dial-in number range defined in the selected *ISDN/PSTN Network Service*. This field cannot be left empty. If left empty an error message, *Please enter the First Dial in Number* is displayed. Length: 0-25 digits. **Note:** This number must be numerically smaller than the *Last Dial-in Number* in the range.
Last Phone Number	Enter the last number in the *Dial-in* number range to be used for dialing into the gateway. This number must be part of the dial-in number range defined in the selected *ISDN/PSTN Network Service*. This field cannot be left empty. If left empty an error message, *Please enter the Last Dial in Number* is displayed. Length: 0-25 digits. **Note:** This number must be numerically larger than the *First Dial-in Number* in the range.
Use Dial-In Numbers as Prefix Range	When selected - *Dial-in* numbers are used to automatically generate the dial string of the destination endpoint or DMA Meeting Room or the IP endpoint, skipping the interaction with the Gateway IVR system for entering the destination ID. For more details see "*Direct Dial-in to Endpoints or DMA VMR using Automatically Generated Destination Numbers"* on page **19-9**. When cleared - The participant must interact with the *IVR Service* to enter the ID of the destination endpoint of the DMA Meeting Room. **Note:** If you enable the ISDN/PSTN access, define these numbers or the dial-in phone number ranges to prevent abuse of the *gateway.*

Table 19-6 *New Gateway Profile Properties (Continued)*

Option	Description
Forward Prefix	Enter the *DMA prefix or the RMX prefix in the Gatekeeper* for use in automatic dial string generation. This prefix replaces the digits that are truncated from the dial-in strings and to which the remaining dial in digits are appended to create the destination number. For example, if the DMA Prefix in the Gatekeeper is 26, enter this prefix in this field.
Number of Digits to Forward	Enter the number of rightmost digits of the dialed string to be appended to the Destination Prefix (*DMA/RMX prefix in the gatekeeper)* when automatically generating the forwarded dial string. For example, if the number of digits to append is 4 and the dialing string is 5705555, the system will append the digits 5555 to the DMA prefix (26) and creates the destination number 265555.

4 Click **OK**.
The new *Gateway Profile* is added to the list.

System Configuration

For details about adding and modifying system flags, see *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Manually Adding and Deleting System Flags"* on page 22-18.

Displaying the Connection Information

You can hide the connection indications displayed on the participant's screen during the connection phase by changing the system configuration and manually adding and setting the system flag **DISABLE_GW_OVERLAY_INDICATION** to **YES** in the MCMS_PARAMETERS_USER tab.

By default, this flag is set to **NO** and all connection indications are displayed.

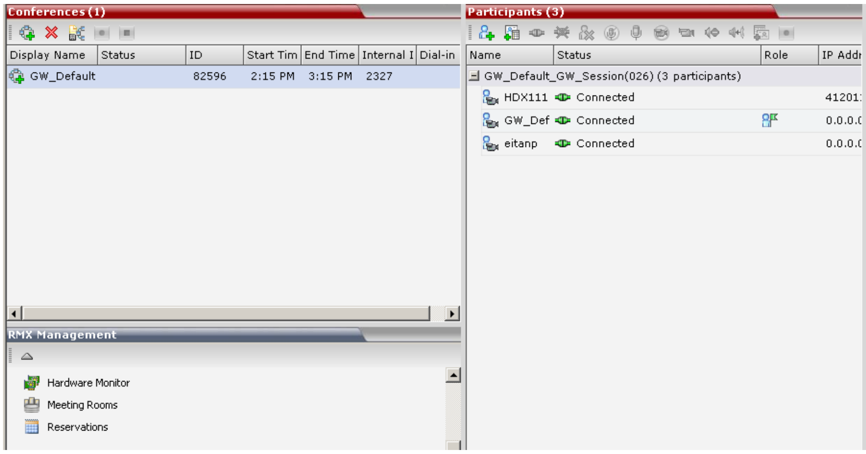
Enabling PSTN dial-in using GK prefix

The feature is enabled when setting the flag **USE_GK_PREFIX_FOR_PSTN_CALLS** to **Yes.**

For more details, see "*Enabling PSTN dial-in using GK prefix"* on page 19-21.

Monitoring Ongoing Gateway Sessions

Ongoing *Gateway Sessions* that are created when calling the Gateway Profile, are listed in the ongoing *Conferences* list pane.



Gateway Sessions are monitored in the same way as the conferences. For more details on monitoring conferences, see *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide*, "*Conference Level Monitoring*" on page **13-3**.

Additional ISDN and PSTN Participants cannot dial in directly to the *Gateway Session* once it was started.

Connection Indications

During the connection process to the other endpoints, the system displays on the calling participant’s screen the called number and the connection status.

A Maximum of 32 characters can be displayed for connection indications. If the displayed information is longer than 32 characters the text is truncated.

If the system dials out to only one destination endpoint, the dialed number is not shown, only the connection status.

If the destination endpoint is ISDN, the system displays the connection progress in percentages, where the percentages represent various stages in the connection process as follows:

- Up to 60% the connection of the ISDN channels (up to 30 channels can be connected when E1 is used for the connection).
- 60% - 80% BONDING stage.
- 80% - 90% Capability exchange stage.
- 90% - 99% Media connection stage.

Once the call is completed, the indications are cleared.

If the call is not completed after trying all possible protocols, the system displays the number that was dialed on the calling endpoint’s screen and one of the following causes:

- *Busy* - the far endpoint is in another call. In such a case, the system does not try to connect using another communication protocol.

- *Rejected* - the far endpoint has rejected the call. In such a case, the system will try to connect using another communication protocol.
- *Unreached* - the number could not be resolved by the gatekeeper or the SIP proxy or could not be found on the network. In such a case, the system will try to connect using another communication protocol.
- *Failed* - any reason causing the system not to complete the connection process. In such a case, the system will try to connect using another communication protocol.

You can hide the connection indications by changing the system configuration. For more details, see "*System Configuration"* on page **19-21**.

Gateway Session Parameters

Gateway Session Name

The RMX creates a new conference that acts as a *Gateway Session* with a unique ID whose display name is composed of the following components:

- The prefix **`GW_`**,
- The *Gateway Profile* display name. For example, `Default_GW_Session`
- `(number)` where the number is a gateway conference counter.

For example: if the *Gateway Profile* display name is Default_GW_Session, the conference name will be GW_Default_GW_Session(001).

Conference ID:

The ID of the new conference is assigned randomly by the MCU.

The *Gateway Session* automatically ends when only one participant is left in the session.

Connected Participant Parameters

Once this conference is created, the calling participant is connected to it and one or several dial-out participant(s) are automatically created and added to this *gateway session*. The dial-in participant is also identified as the chairperson of the conference.

The connecting (dial-in) participant name is taken from the endpoint. If the endpoint does not send its name, it is derived from the Gateway Profile display name and it includes the *Gateway Session* name, underscore and a random number is displayed (between brackets), for example, `GW_Default_GW_Session(001)_(000)`.

The name of the destination (dial-out) participant is taken from the endpoint. If the endpoint does not send its name, it is taken from the dialed number. If the dialed number was an IP address, the system displays underscores instead of dots, for example, `172_22_172_89`.

Participants connected to a *gateway session* are monitored in the same way as participants connected to ongoing conferences. For details, see *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Participant Level Monitoring"* on page **13-21**.

Direct Dialing from ISDN/PSTN Endpoint to IP Endpoint via a Meeting Room

Dialing from an ISDN endpoint to a specific IP endpoint using the Gateway Profile is a two-step process (dialing to the Gateway and then entering the number of the destination IP endpoint).

When dialing to specific IP endpoints you can simplify the dialing process by creating the appropriate Meeting Room.

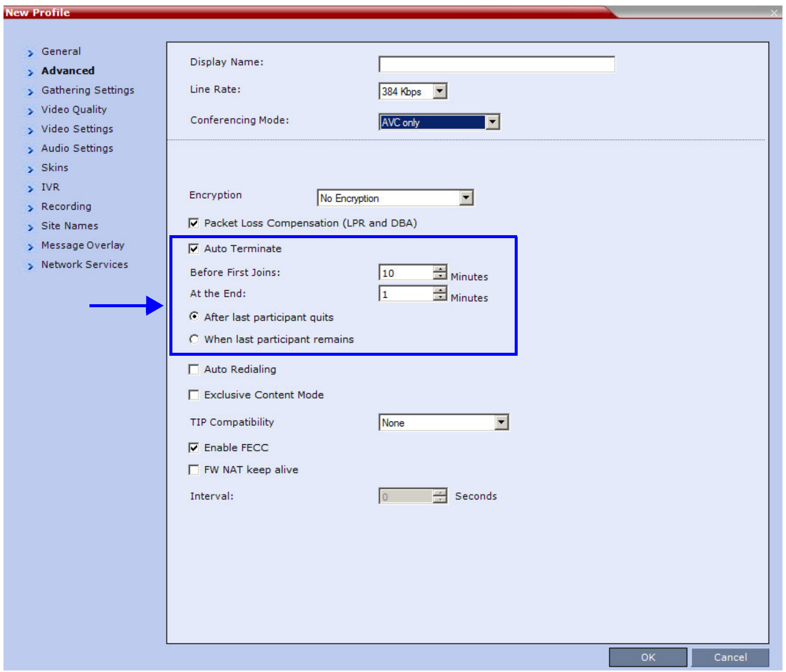
If CMA is involved, dialing can be simplified even further by configuring the appropriate dialing Rule in the CMA.

To set up the Meeting Room for direct dialing in:

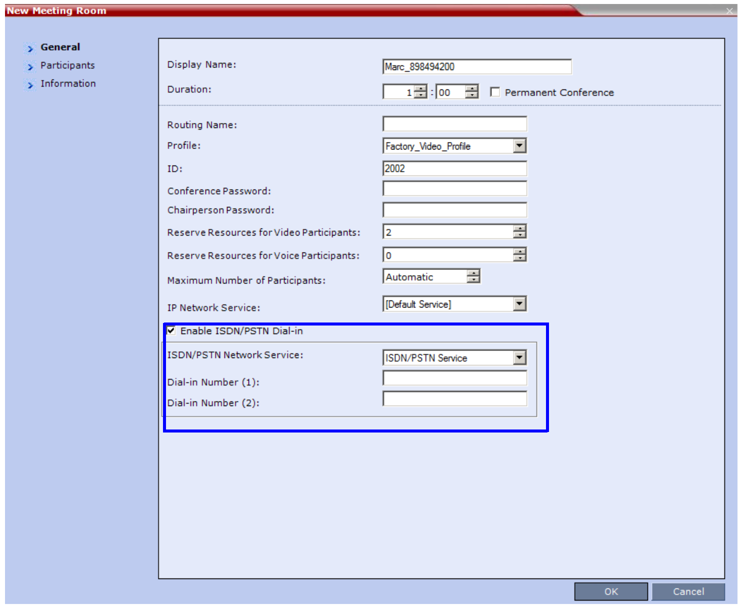
Set the conference parameters in the Conference Profile and make sure that the conference will automatically end when there is only one participant connected to the meeting.

Define the Meeting Room with the following:

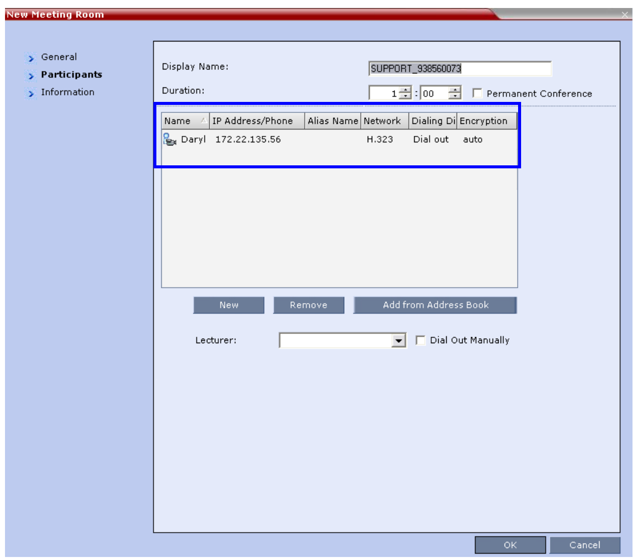
- Conference Profile in which the **Auto Terminate - At the end - When Last Participant Remains** option is selected. For more details on Conference Profile definition, see *"Defining the IVR Service for Gateway Calls"* on page **19-14**.



- ISDN/PSTN access is enabled and a dial-in number is assigned to the Meeting Room.



- The dial-out IP endpoint is added to the Meeting Room's Participants list.



Dialing to Polycom® DMA™ 7000

Two dialing methods are available to ISDN/PSTN participants calling the DMA:

- Direct with automatically generated destination dial strings from dial-in strings. This option is available only from version 7.1 and only to RMX with MPM+ and MPMx cards.
- Via Gateway IVR.

In addition, PSTN participants can dial the Gateway IVR and can use the MCU or DMA prefix in the gatekeeper together with the conference ID/endpoint alias as the destination string to simplify the input. This is one of the methods for PSTN participants to connect to a virtual Meeting Room on the DMA. For more details, see "*PSTN Dial-in Using GK Prefix"* on page **19-9**.

Calling a DMA Direct with Automatically Generated Destination Dial Strings

In this configuration, the gateway session initiator enters one of the dial-in numbers assigned to the gateway profile. This number is truncated by the RMX gateway and the truncated digits are replaced by a prefix that corresponds either to the DMA prefix in the Gatekeeper.

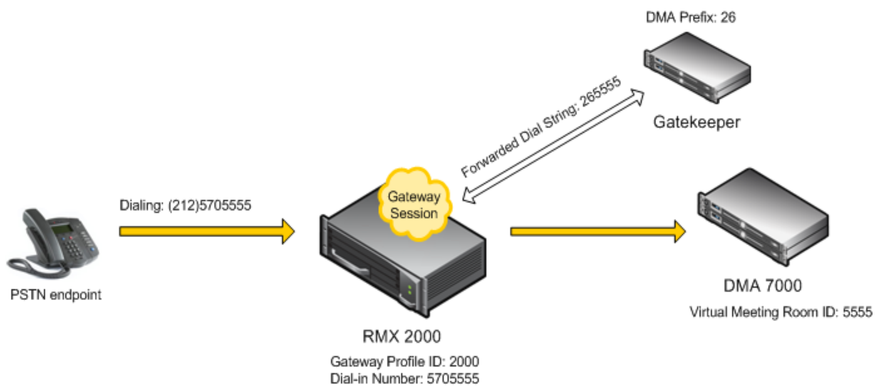


Figure 21 *Call Flow from ISDN Endpoint to Polycom DMA with Automatically Generated Forwarded Dial String*

Example:

Figure 1 shows the call flow assuming the following parameters:

First Dial-in Number	5705550
Last Dial-in Number	5705560
Use Dial-in Numbers as Destination ID	Selected
DMA Meeting Room ID	5555
Destination Prefix (DMA prefix in Gatekeeper)	26
Number of Rightmost Digits to Append	4
PSTN participant dials	(212)5705555
Number that will be used by RMX to forward the call to the DMA	265555

Calling the DMA via Gateway IVR

Audio PSTN/ISDN calls can be routed to Polycom DMA 7000 via the RMX. ISDN Video endpoints connect using their audio channels (but consume video resources). The DMA 7000 enables load balancing and the distribution of multipoint calls on up to 10 Polycom RMX media servers.

As part of this solution, the RMX acts as a gateway for the DMA that supports H.323 calls. The PSTN or ISDN endpoint dials the virtual Meeting Room on the DMA via the Gateway Profile on the RMX.

Both the RMX and the DMA must be registered with the same gatekeeper.

The dialing string of the destination conference on the DMA must be communicated to the dialing endpoint and used during the connection to the Gateway Profile on the RMX. There are two options available for doing this:

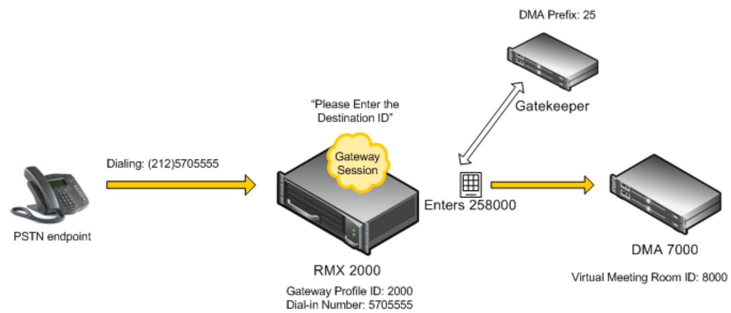
- Manual Dial String Entry
- Automatic Dial String Generation (*MPM*+ and *MPMx* cards only)

Manual Dial String Entry

Figure 19-1Dialing String and Call Flow from ISDN Endpoint to Polycom DMA

The connection is done in two steps:

- A PSTN/ISDN participant dials the dial-in number assigned to the Gateway Profile (5705555), including the country and area code (if needed) and connects to the Gateway IVR.
- When prompted for the target conference ID, the caller enters the string of the target meeting room on the DMA followed by the # key.



This string is composed of the DMA prefix as registered in the gatekeeper and the ID of the virtual meeting room running on the DMA. For example, if the DMA prefix is 25 and the target meeting room ID is 8000 the participant enters 258000 followed by the # key.

The RMX creates a *Gateway Session* with two participants, the calling participant and the link to the conference running on the DMA.

Automatic Dial String Generation

The administrator can configure the *Gateway Profile* to automatically generate and forward the dial string from the *RMX Gateway Session* to the *DMA* in order to connect to the required *DMA Meeting Room*. When this configuration option is selected, the participant does not need to interact with the *IVR Service*.

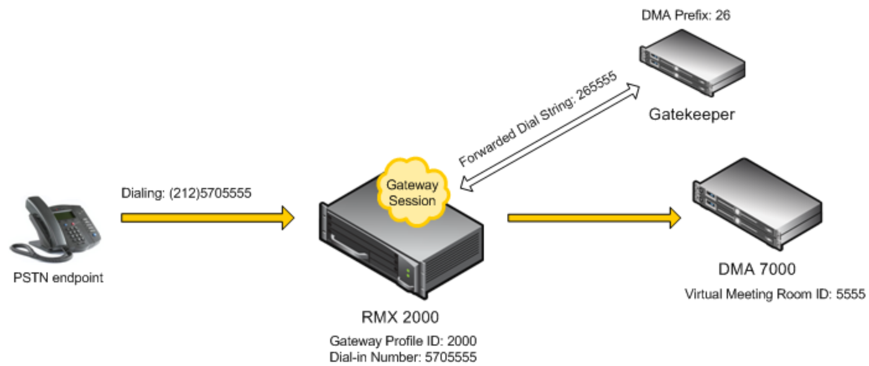


Figure 20 *Call Flow from ISDN Endpoint to Polycom DMA with Automatically Generated Forwarded Dial String*

Example:

Figure 1 shows the call flow assuming the following parameters:

First Dial-in Number	5705550
Last Dial-in Number	5705560
Use Dial-in Numbers as Destination ID	Selected
PSTN participant dials	(212)5705555
Destination Prefix (DMA Gatekeeper)	26
Number of Rightmost Digits to Append	4
DMA Meeting Room ID	5555

PSTN Dial-in Using GK Prefix

When connecting to an RMX that is standalone or part of a *DMA* solution deployment, *PSTN* participants are prompted by an *IVR* message requesting the *Destination Conference ID* followed by the **#** key to be entered using the *DTMF* input keypad.

Including the *Gatekeeper Prefix* in the *DTMF* input string enables *PSTN* participants to use the input string when connecting to an RMX whether the RMX is a standalone *MCU* or part of a *DMA* solution deployment.

Enabling PSTN dial-in using GK prefix

The feature is enabled by the **USE_GK_PREFIX_FOR_PSTN_CALLS** *System Flag* in *system.cfg*. For more information see "*Modifying System Flags"* on page **22-1**.

Table 19-7 summarizes the *PSTN* participant's *DTMF* input depending on the flag value.

Table 19-7 *PSTN Participant input via DTMF*

Configuration	**FLAG: USE_GK_PREFIX_FOR_PSTN_CALLS=**	
	NO	**YES**
Standalone RMX Conference ID= 1234	PSTN participant enters: **1234#**.	PSTN participant enters: **761234#** (The *Gatekeeper Prefix*"**76**" is automatically removed from the DTMF input string for a standalone RMX.)
RMX with DMA Virtual Meeting Room ID in DMA = 1234 DMA gatekeeper prefix = 76	PSTN participant enters: **761234#**	

Deploying a Polycom RMX™ Serial Gateway S4GW

UC APL Public Key Infrastructure (*PKI*) requires that the *Serial Gateway S4GW* be connected directly to the RMX and not to the *H.323* network. The *Serial Gateway* effectively becomes an additional module of the RMX, with all web and *H.323* traffic passing through the RMX.

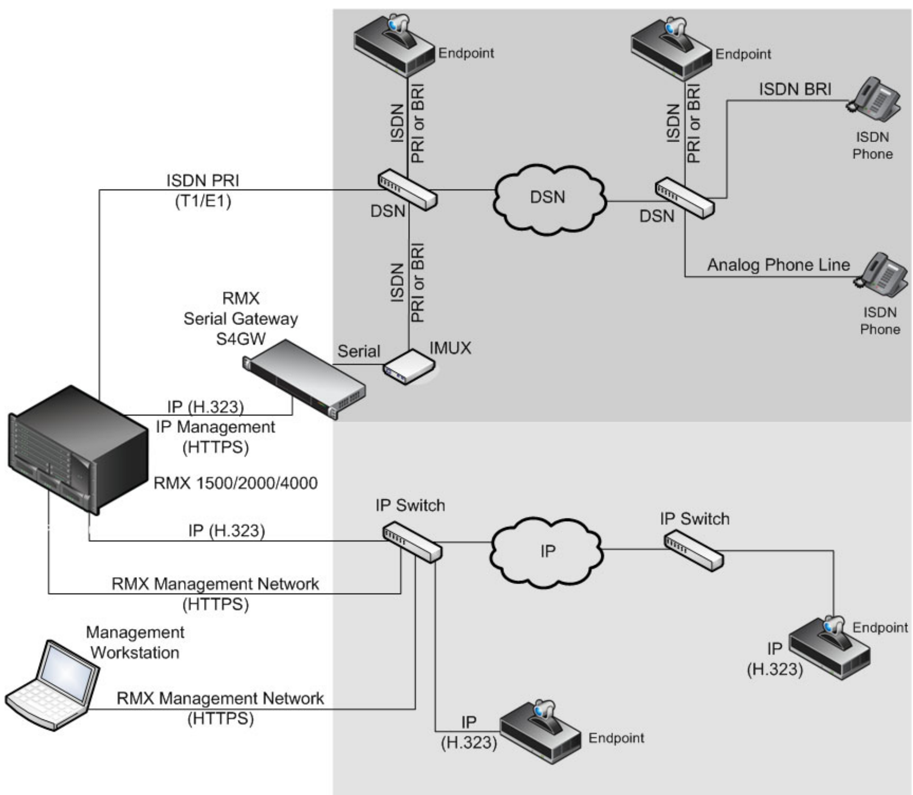


Figure 19-1*Network infrastructure with direct connection to Serial Gateway S4GW*

For more information see the *Polycom RealPresence Collaboration Server (RMX) 1500/2000/4000™ 1500/2000/4000 Deployment Guide for Maximum Security Environments*, *"Deploying a Polycom RMX™ Serial Gateway S4GW"* on page **5-1**.

20

RMX Manager Application

The *RMX Manager* is the Windows version of the *RealPresence Collaboration Server Web Client*. It can be used instead of the *RealPresence Collaboration Server Web Client* for routine RMX management and for RMX management via a modem connection. For more information on using the *RMX Manager* via a modem connection, see "*Connecting to the MCU via Modem"* on page **G-7**.

Using the *RMX Manager* application, a single user can control a single or multiple MCU units as well as conferences from multiple MCUs. The RealPresence Collaboration Server (RMX) system can be managed and controlled by the RMX Manager application.

The RMX Manager can list and monitor:

- Up to 20 RealPresence Collaboration Server (RMX) systems in the MCUs pane
- Up to 800 conferences in the Conferences pane
- Up to 1600 participants in the Participants pane

The *RMX Manager* is faster than the *RealPresence Collaboration Server Web Client* and can give added efficiency to RealPresence Collaboration Server management tasks, especially when deployed on workstations affected by:

- Lack of performance due to bandwidth constraints within the LAN/WAN environment.
- Slow operation and disconnections that can be caused by the anti-phishing component of various antivirus applications.

> Users with *Auditor* authorization level cannot connect to the RMX via the *RMX Manager* application and must use the *RealPresence Collaboration Server Web Client*.

The *RMX Manager* application can be installed in your local workstation or accessed directly on the RealPresence Collaboration Server system without installing it in your workstation.

Accessing the RMX Manager Directly

To access the RMX Manager directly:

>> Start Internet Explorer and in your browser enter: **http://<RMX IP Address>/RMXManager.html**.

For example, if the RMX IP address is 10.226.10.46, enter in the browser the following address: ***http://10.226.10.46/RMXManager.html.***

Installing the RMX Manager

The *RMX Manager* application can be downloaded from one of the RealPresence Collaboration Server systems installed in your site or from Polycom web site at http://www.polycom.com/support.

Upgrade Notes

- When upgrading the *RMX Manager* application, it is recommended to backup the MCU list using the **Export RMX Manager Configuration** option. For more details, see "*Import/Export RMX Manager Configuration"* on page **20-21**.
- When upgrading the *RMX Manager* from a major version (for example, version 7.0) to a maintenance version of that version (for example, 7.0.x), the installation must be performed from the same MCU (IP address) from which the major version (for example, version 7.0) was installed.
  If you are upgrading from another MCU (different IP address), you must first uninstall the *RMX Manager* application using **Control Panel > Add or Remove Programs**.

New RealPresence Collaboration Server (RMX) Installation Note

The *RealPresence Collaboration Server (RMX) Installation and First Entry Configuration* must be completed before installing the *RMX Manager* application. For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "First Time Installation and Configuration".

Once the connection to the RealPresence Collaboration Server (RMX) unit is established and the *Login* window is displayed, the *RMX Manager* application can be installed.

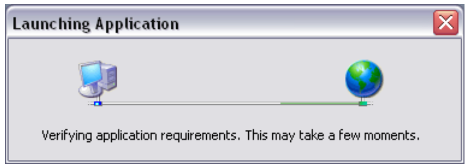
To install RMX Manager (downloading the application from the RealPresence Collaboration Server (RMX)):

1 Start Internet Explorer and connect to one of the RMX units in your site. It is recommended to connect to the RMX installed with the latest software version.

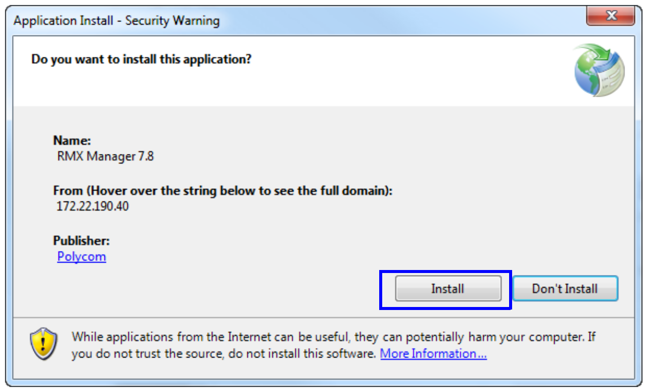
The *Login* screen is displayed. There is a link to the *RMX Manager Installer* at the top of the right edge of the screen.

2 Click the **Install RMX Manager** link.

The installer verifies the application’s requirements on the workstation.

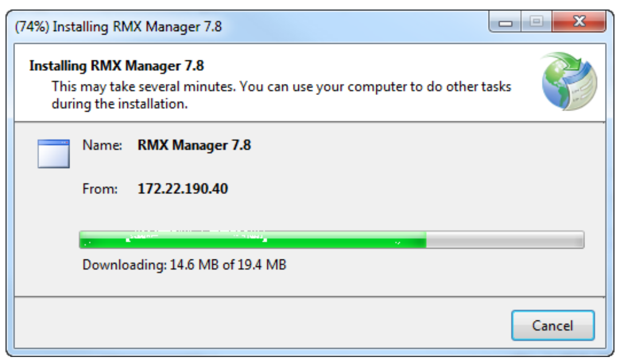


The *Install* dialog box is displayed.

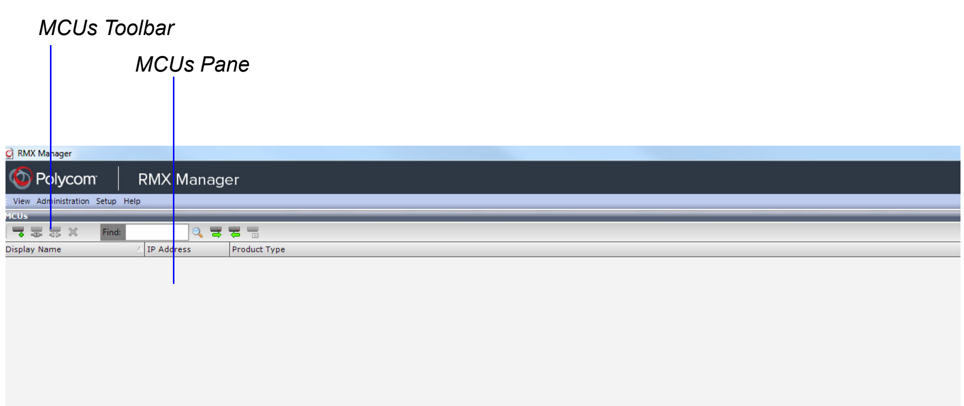


3 Click **Install**.

The installation proceeds.



The installation completes, the application loads and the *RMX Manager - MCUs* screen is displayed.



The first time you start the *RMX Manager* application, the *MCUs* pane is empty.

Starting the RMX Manager Application

Once installed, the *RMX Manager* can be run using the **http://** (non-secured) or **https://** (secured) command in the browser’s address line or the Windows *Start* menu.

To use the browser:

1 In the browser’s command line, enter:

```
http://<MCU Control Unit IP Address>/RMXManager.html
```

or

```
https://<MCU Control Unit IP Address>/RMXManager.html
```

2 Press **Enter**.

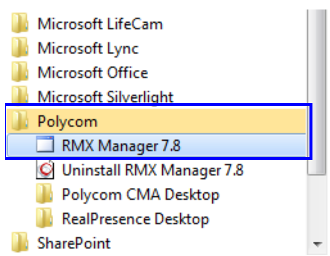
To use the Windows Start menu:

1 Click **Start > Programs.**

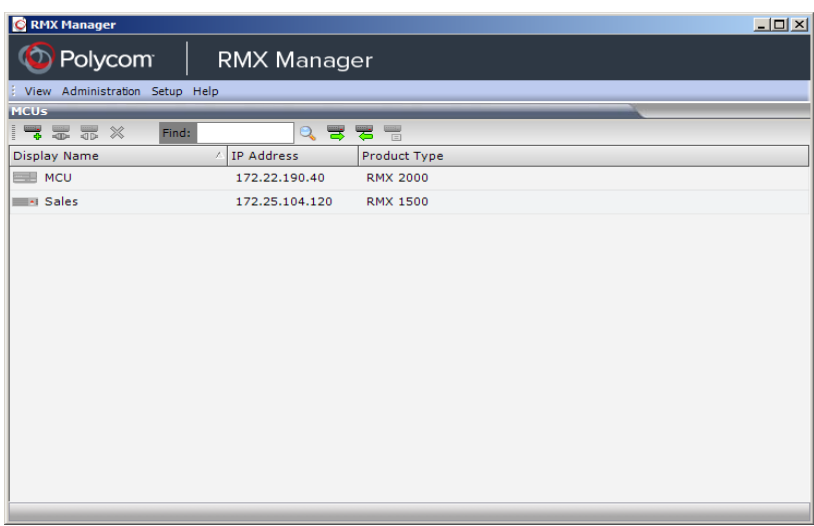
a If the *RMX Manager* is displayed in the recently used programs list, click **RMX Manager** in the list to start the application.

or

b Click **All Programs** > **Polycom** > **RMX Manager**.



The *MCUs* screen is displayed, listing the MCUs currently defined in the *RMX Manager*.



This screen enables you to add additional MCUs or connect to any of the MCUs listed. For details on adding MCUs, see *“Adding MCUs to the MCUs List”* on page 12.

For each listed MCU, the system displays the following information:

— MCU *Display Name* (as defined in the Add MCU dialog box).

— *IP Address* of the MCU’s control unit

— *Product Type* - The MCU type: RealPresence Collaboration Server (RMX) 1500/ RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000.
  Before connecting to the MCU for the first time, the RMX type is unknown so "RMX" is displayed instead as a general indication.

To display the *RMX Manager* main screen you must connect to one of the listed RMXs. For more details, see "*Connecting to the MCU"* on page **20-5**.

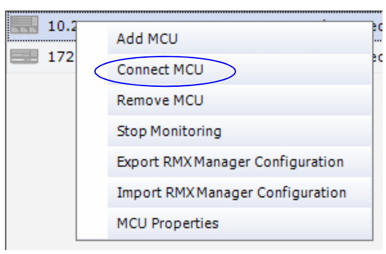
Connecting to the MCU

Once an MCU is defined, the *RMX Manager* can be connected to it. This allows you to set up conferences, make reservations, monitor On Going Conferences and perform other activities on several MCUs.

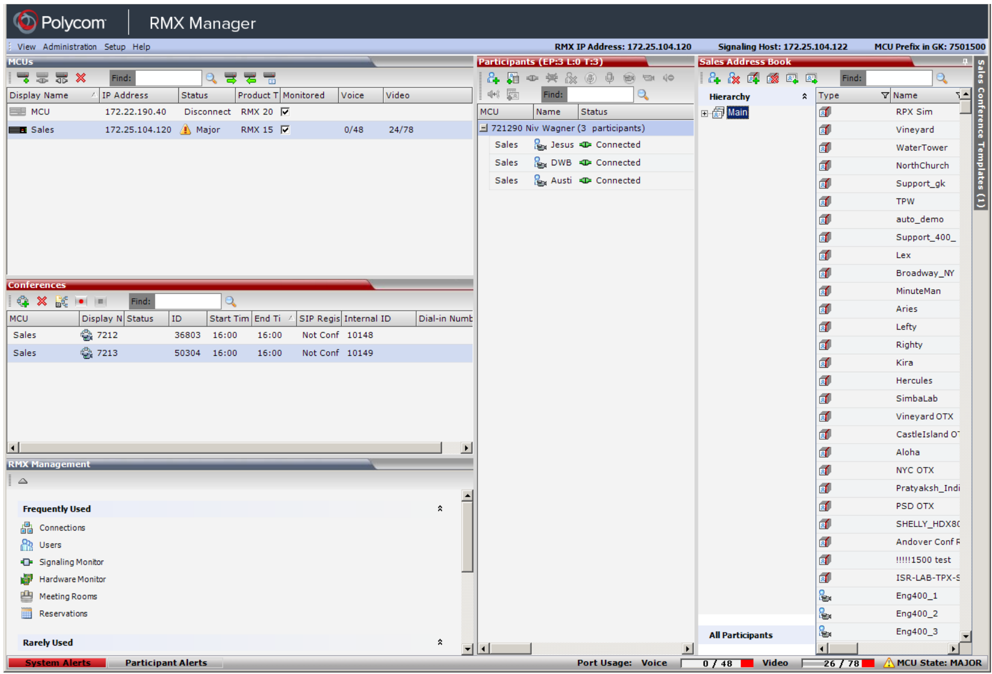
> The first RMX unit that is connected to the *RMX Manager* dictates the Authorization Level of Users that can connect to the other MCUs on the list. For example, if the Authorization level of the User POLYCOM is Administrator, all Users connecting to the other MCUs on the list must be Administrators. Each user can have a different login name and password for each of the listed MCUs and they must be defined in the Users list of each of the listed MCUs.

To connect the RMX Manager to an MCU:

1 In the *MCUs* pane or screen, use one of the following methods:
   a Double-click the MCU icon.
   b Select the RMX to connect and click the **Connect MCU** button.
   c Right-click the MCU icon and then click **Connect MCU**.

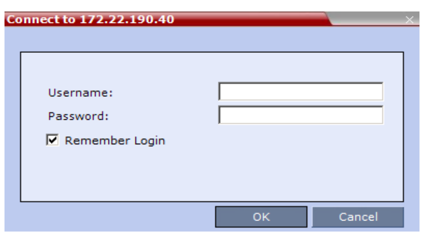


If you are connecting to the MCU from the *MCUs* opening screen and have defined the *Username* and *Password* for the connecting MCU, the system connects to the RMX, and the *RMX Manager Main Screen* is displayed.



If you are connecting to any MCU from the *MCUs* pane in the *RMX Manager Main Screen* and have defined the *Username* and *Password* for the connecting MCU, the MCU icon changes to connected and its status, type and number of audio and video resources are displayed in the *MCUs* pane.

If the *Username* and *Password* are missing from the MCU parameters, or if the *Remember Me* check box has been cleared, the *Connect* dialog box opens.



2 In the *Username* field, enter the user name with which you will login to the MCU.

3 In the *Password* field, enter the password as defined for the user name with which you will login to the MCU.

4 To add the user name and password to the MCU properties so you will not have to enter them each time you login to the MCU, make sure that the **Remember Login** check box is selected. Otherwise, clear the **Remember Login** check box.

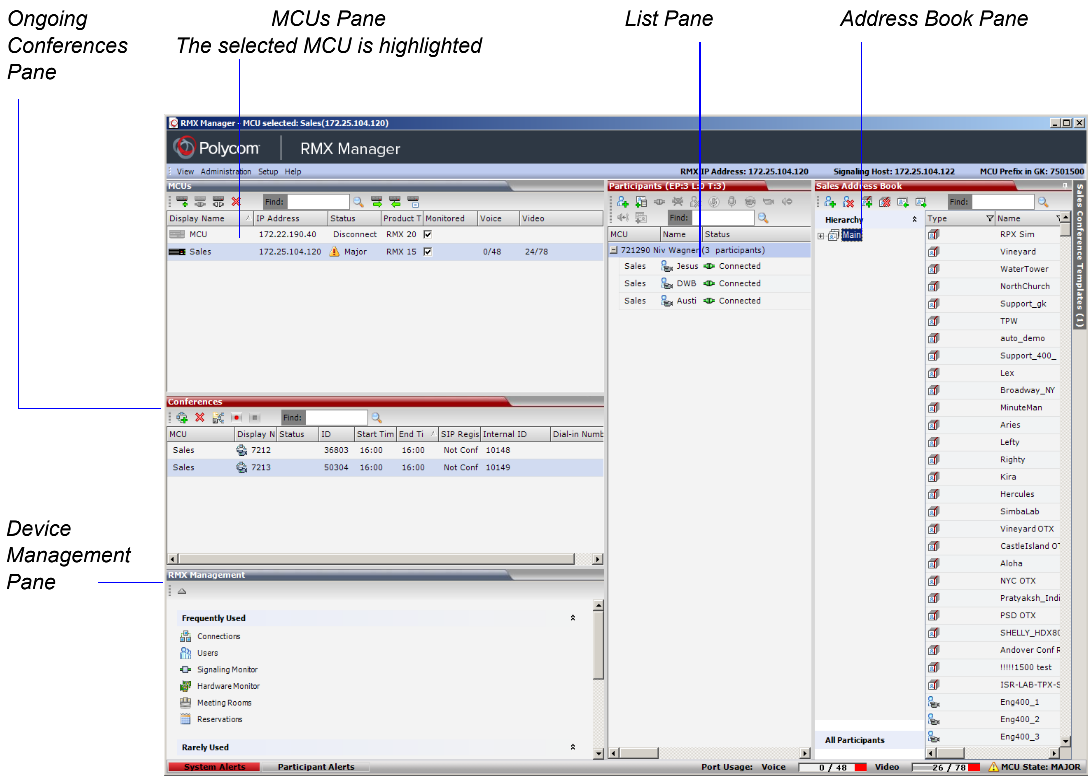
5 Click **OK**.
The system connects to the RMX, and the *RMX Manager Main Screen* is displayed.

If a User with the entered *Username* and *Password* is not defined in the RMX, an error message is displayed and the system lets you re-enter the *Username* and *Password.*

RMX Manager Main Screen

The *RMX Manager Main Screen* is displayed only when at least one MCU is connected.

This screen is similar to the *RealPresence Collaboration Server Web Client Main Screen* with the addition of the *MCUs* pane. As in the *RealPresence Collaboration Server Web Client*, the panes are displayed according to the *Authorization Level* of the logged in User. The *MCUs* pane is displayed to all users.

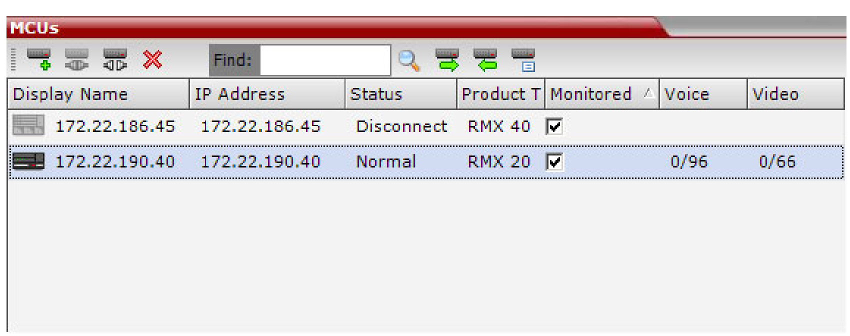


Only one MCU can be selected in the *MCUs* pane. If only one MCU is connected, it is automatically selected. The selected MCU is highlighted.

The menu items, the *RMX Management* features, the *Address Book* and the *Conference Templates* are all properties of the selected MCU and apply to it.

MCUs Pane

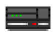
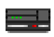
The MCUs pane includes a list of MCUs and a toolbar.



For each listed MCU, the system displays the following information:

- MCU *Display Name* - the name of the MCU and its icon according to its type and connection status. The following icons are available:

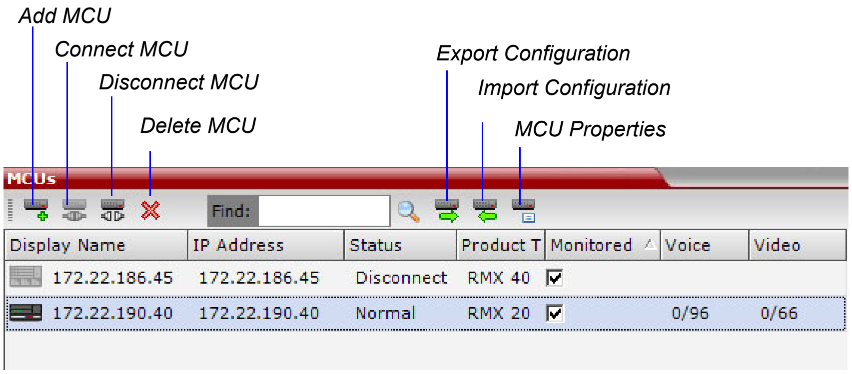
Table 20-1 *MCU Icons and Statuses*

Icon	Description
	RealPresence Collaboration Server (RMX) 1500, disconnected.
	RealPresence Collaboration Server (RMX) 1500, connected.
	RealPresence Collaboration Server (RMX) 2000, disconnected.
	RealPresence Collaboration Server (RMX) 2000, connected.
	RealPresence Collaboration Server (RMX) 4000, disconnected.
	RealPresence Collaboration Server (RMX) 4000, connected.

- *IP Address* of the MCU’s control unit.
- *Status* - The status of the MCU:
  — *Connected* - the MCU is connected to the *RMX Manager* and can be managed by the *RMX Manager* user.
  — *Disconnected* - The MCU is disconnected from the *RMX Manager*
  — *Major* - The MCU has a major problem. MCU behavior could be affected and attention is required.
- *Product Type* - The MCU type: RealPresence Collaboration Server 1500/2000/4000. Before connecting to the MCU for the first time, the RMX type is unknown so RMX is displayed instead as a general indication.
- *Monitored* - When checked indicates that the conferences running on this MCU are automatically added to the *Conferences* list and monitored. To stop monitoring the conferences running on this MCU and their participants, clear the *Monitored* check box.
- *Video Resources* - The number of video resources that are available for conferencing.
- *Audio Resource*s - The number of audio resources that are available for conferencing.

MCUs Toolbar

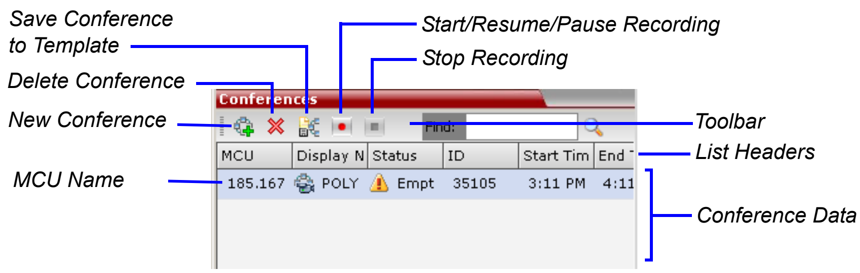
The *MCUs* toolbar contains the following buttons:



Conferences Pane

The *Conferences* pane lists all the ongoing conferences from all the MCUs that are connected and monitored along with their *MCU*, *Status*, *Conference ID*, *Start Time* and *End Time* data. The number of ongoing conferences is displayed in the pane's title.

The *Conferences* list toolbar contains the following buttons:



If *Conference Recording* is enabled the following buttons are enabled:

- *Start/Resume Recording* – start/resume recording.
- *Stop Recording* – stop recording.
- *Pause* – toggles with the *Start/Resume* button.

Monitoring conferences

New conferences run on MCUs selected for *Monitoring* are automatically added to the *Conferences* list. You can sort the conferences by MCU by clicking the **MCU** column heading in the *Conferences* table. Conferences run on MCUs that are connected but not monitored are not listed.

Using Windows multiple selection methods to select conferences, participants from several conferences running on different MCUs can be listed in the *Participants* list pane.

Starting a new conference

When starting a new conference, you must first select the MCU to run the conference in the MCUs pane.

RMX Management

The *RMX Management* pane lists the entities **of the selected MCU** that need to be configured to enable the RMX to run conferences. Only users with Administrators permission can modify these parameters.

The *RMX Management* pane is divided into two sections:

- **Frequently Used** – parameters often configured monitored or modified.
- **Rarely Used** – parameters configured during initial system set-up and rarely modified afterward.

List Pane

The *List* pane displays details of the participants connected to the conferences selected in the *Conferences* pane or the item selected in *RMX Management* pane. The title of the pane changes according to the selected item.

When selecting an item in the *RMX Management* pane it applies only to the MCU selected in the MCUs list. In such a case, the system displays the name of the selected MCU in the List pane title.

Status Bar

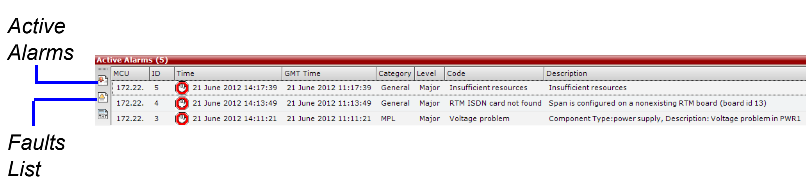
The *Status Bar* at the bottom of the *RealPresence Collaboration Server Web Client* contains *System* and *Participant Alerts* tabs as well as *Port Usage Gauges* and an *MCU State* indicator.

System Alerts

Lists system problems of all connected MCUs (even if the MCU is not monitored). The alert indicator flashes red when at least one system alert is active. The flashing continues until a user with Operator or Administrator permission reviews the list.

The *System Alerts* can be sorted by MCU by clicking the *MCU* header in the *System Alerts* table.

The *System Alerts* pane is opened and closed by clicking the **System Alerts** button in the left corner of the *Status Bar*.



For more information about **Active Alarms** and **Faults List,** see "*System and Participant Alerts"* on page **21-1**.

Participant Alerts

Lists the participants of all monitored MCUs that are experiencing connection problems. The list is sorted by MCU and conference.

The *Participant Alerts* can be sorted by MCU by clicking the *MCU* header in the *Participant Alerts* table.

The *Participant Alerts* pane is opened and closed by clicking the **Participant Alerts** button in the left corner of the *Status Bar*.

Port Usage Gauges

The *Port Usage* gauges display for the selected MCU:

- The total number of *Video* or *Voice* ports in the system according to the *Video/Voice Port Configuration*. The *Audio* gauge is displayed only if *Audio* ports were allocated by the administrator, otherwise only the *Video* port gauge is displayed.
- The number of *Video* and *Voice* ports in use.
- The *High Port Usage* threshold.

For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Port Usage Gauges"* on page **3-6**.

MCU State

The *MCU State* indicator displays the status of the selected MCU.

For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*MCU State"* on page **3-7**.

Address Book

Displays the *Address Book* of the **selected** MCU (regardless of its *Monitored* status). The *Address Book* is a list of *Participants* and *Groups* that have been defined on the **selected** RMX.

The information in the *Address Book* can be modified only by an administrator. All RMX users can, however, view and use the *Address Book* to assign participants to conferences.

The name of the selected RMX is displayed in the title of the Address Book pane. For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Address Book"* on page **3-8**.

Conference Templates

Conference Templates enable administrators and operators to create, save, schedule and activate identical conferences.

The *Conference Templates* pane lists the Conference Templates that have been defined on the **selected** RMX (regardless of its *Monitored* status).

The *Conference Templates* pane is initially displayed as a closed tab. The name of the selected RMX and the number of saved *Conference Templates* is indicated on the tab.

For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Conference Templates"* on page **3-9**.

Adding MCUs to the MCUs List

The *RMX Manager* can connect to one or several RMXs simultaneously. If the site's configuration includes more than one MCU, or when a new MCU is added to your configuration, and you want to monitor and control all MCUs from within the same window, you must add the MCU to the MCUs list.

> The RMX must be installed and its IP addresses properly configured in the Management Network Service before defining its connection parameters in the *RMX Manager* application.

To add the MCU to the list of MCUs being managed, define the MCU's connection parameters.

To add a RMX unit:

1 On the *MCUs* toolbar, click the **Add MCU**  button to add an MCU to the MCU list. The *Add MCU* dialog box opens.

2 Define the following parameters:

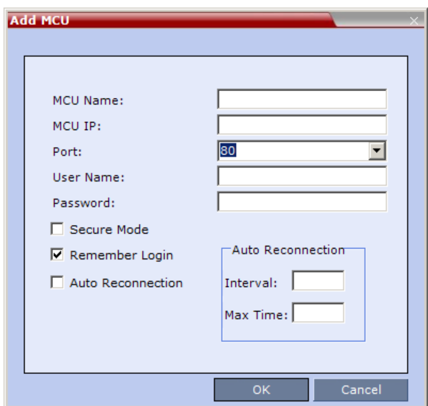


Table 21 *MCU Properties*

Field	Description
MCU Name	Enter the name of the MCU on the network.
MCU IP	Enter the IP address of the MCU's Control Unit. The IP address must be identical to the one configured in the MCU during first entry Configuration. For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Modifying the Factory Default Management Network Settings on the USB Key"* on page **2-6**.
Port	Enter the number of the port used for communication and data transactions between the RMX unit and the *RMX Manager*. For standard connection, enter **80**. For a Secured connection (using TLS or SSL), enter **443**.
Username	Enter the user name with which you will login to the MCU. A User with this name must be defined in the RMX Users list. The system is shipped with a default User whose name is POLYCOM.

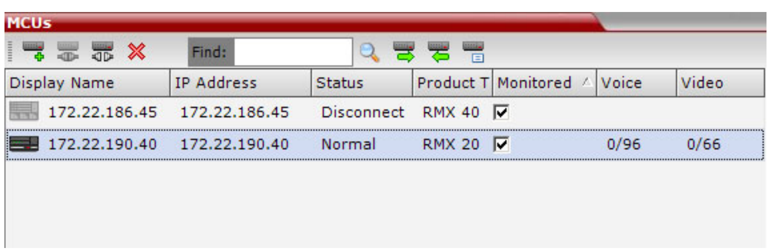
Table 21 *MCU Properties (Continued)*

Field	Description
Password	Enter the password as defined for the user name with which you will login to the MCU. The system is shipped with a default User whose password is POLYCOM.
Secure Mode	**Optional**. Select this check box to connect to the RMX with SSL and work in Secure Mode.
Remember Login	This check box is automatically selected, and it enables the usage of the user name and password entered in this dialog box when connecting to the RMX. If this check box is cleared, the user is prompted for the user name and password when connecting to this RMX unit.
Auto Reconnection	Select this check box to automatically reconnect to the RMX if the connection between the *RMX Manager* and the MCU is broken.
Interval	Enter time in seconds between reconnect ion attempts to the RMX. For example, if you enter 10, the system will wait 10 seconds between the connection attempts.
Max Time	Enter the maximum amount of time in seconds that the RMX is allowed to try to reconnect. If the RMX reconnects before the allotted time frame the count down timer is halted. For example, if you enter 100, the system will stop trying to reconnect if it has failed to do so within 100 seconds.

3 Click **OK**.
The MCU is added to the MCUs pane.

4 If required, repeat steps 1-3 to define additional RMX units.

The *MCUs* pane contains the list of all defined MCUs.



Starting a Conference

There are several ways to start a conference:

- Clicking the *New Conference* button in the *Conferences* pane. For more information, see *"Starting a Conference from the Conferences Pane"* on page **14**.
- Dialing in to a Meeting Room defined on any of the MCUs.
  — A Meeting Room is a conference that is saved on the MCU. It remains in passive mode until it is activated by the first participant, or the meeting organizer dialing in. For more information about Meeting Rooms, see "*Meeting Rooms"* on page **6-1**.

- Dialing in to an Ad Hoc Entry Queue defined on one of the MCUs which is used as the access point to the MCU.

  For a detailed description of Ad Hoc Entry Queues, see "*Entry Queues"* on page **7-1**.
- Start a *Reservation:*
  - — If the *Start Time* of the *Reservation* is past due the conference becomes ongoing immediately.
  - — If the *Start Time* of the *Reservation* is in the future the conference becomes ongoing, at the specified time on the specified date.

  For more information, see "*Starting a Reservation"* on page **20-15**.
- Start any *Conference Template* saved in the *Conference Templates* list.
  For more information, see "*Starting an Ongoing Conference or Reservation From a Template"* on page **20-16**.

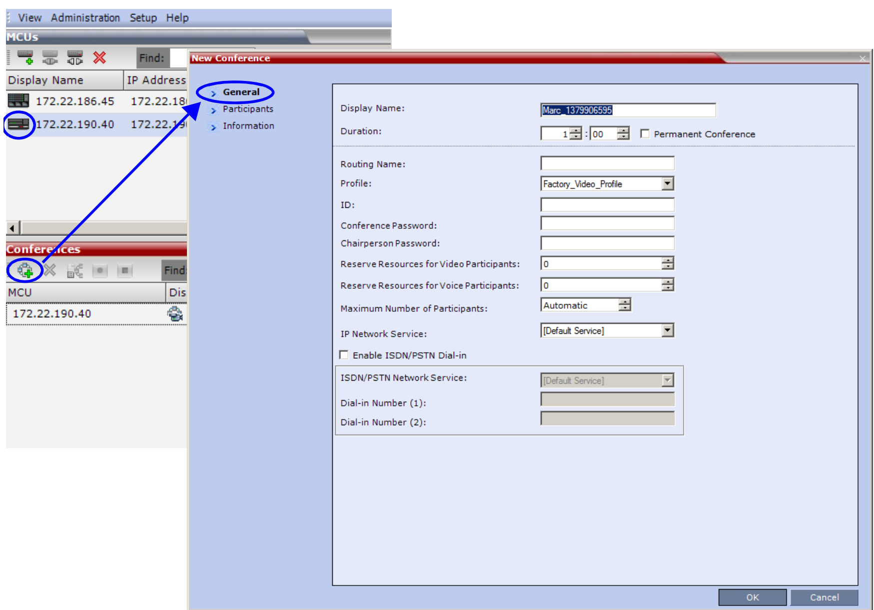
Starting a Conference from the Conferences Pane

To start a conference from the Conference pane:

1 In the *MCUs* pane, select the MCU to run the conference.

2 In the *Conferences* pane, click the **New Conference** ( ) button.

The *New Conference – General* dialog box opens.



The system displays the conference’s default *Name*, *Duration* and the default *Profile*, which contains the conference parameters and media settings.

The RMX automatically allocates the conference *ID*, when the conference starts.

In most cases, the default conference *ID* can be used and you can just click **OK** to launch the conference. If required, you can enter a conference *ID* before clicking **OK** to launch the conference.

If you are the meeting chairperson or organizer using the *RealPresence Collaboration Server Web Client* to start your own meeting, you need to communicate the default conference ID (or the one you created) to the other conference participants so they can dial in.

You can use the *New Conference - General* dialog box to modify the conference parameters. If no defined participants are to be added to the conference, or you do not want to add additional information, click **OK**.

For more details, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Starting an AVC Conference from the Conferences Pane"* on page **3-13**.

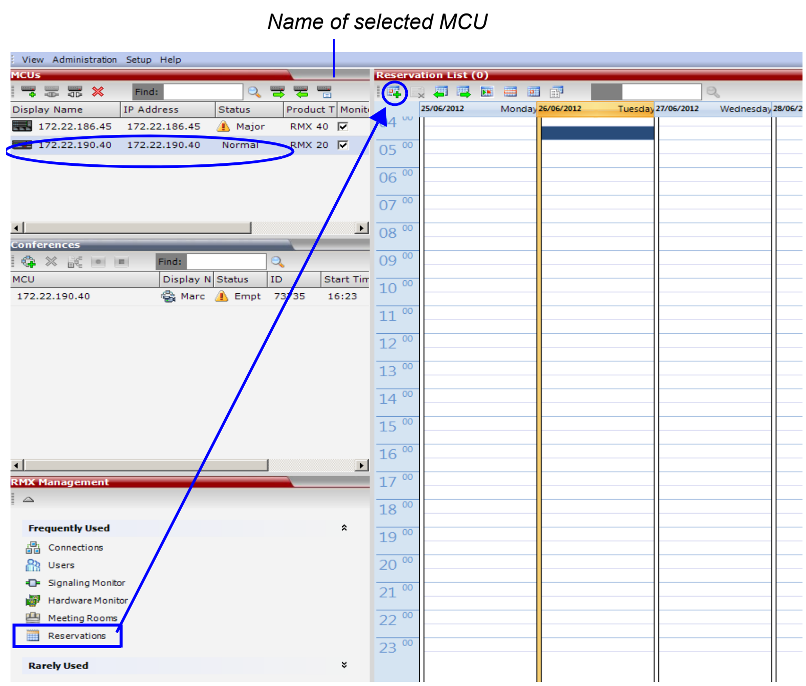
Starting a Reservation

To start a conference from the Reservation Calendar:

1 In the *MCUs* pane, select the MCU to run the conference.

2 In the *RMX Management* pane, click the *Reservation Calendar* button ( ).

The *Reservation Calendar* is displayed.



3 Click the **New Reservation** ( ) button.

For more information, see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Changes made to this information once the conference is running are not saved to the CDR."* on page **3-24**.

Starting an Ongoing Conference or Reservation From a Template

An ongoing conference or a Reservation can be started from any Conference Template saved in the *Conference Templates* list of the selected MCU.

To start an ongoing conference or a reservation from a Template:

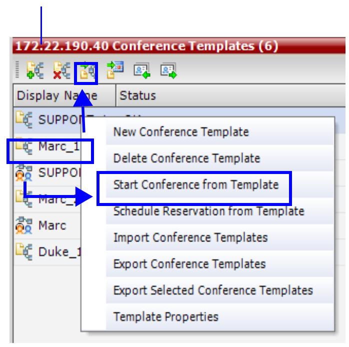
1 In the *MCUs* pane, select the MCU to run the conference.

1 In the *Conference Templates* list, select the Template you want to start as an ongoing conference.

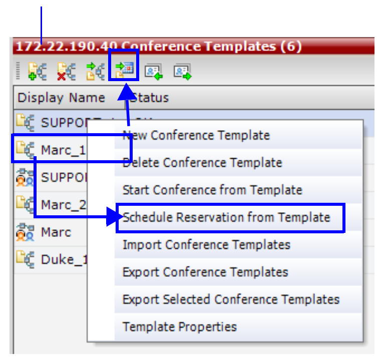
2 Click the **Start Conference from Template** ( ) button to start a conference or

Schedule Reservation from Template ( ) button to schedule a reservation.
or
Right-click and select **Start Conference from Template** to start an ongoing conference or **Schedule Reservation from Template** to schedule a reservation.

Name of selected MCU



Name of selected MCU



The conference is started.

For detailed description of *Conference Templates*, see "*Conference Templates”* on page **11-1**.

Monitoring Conferences

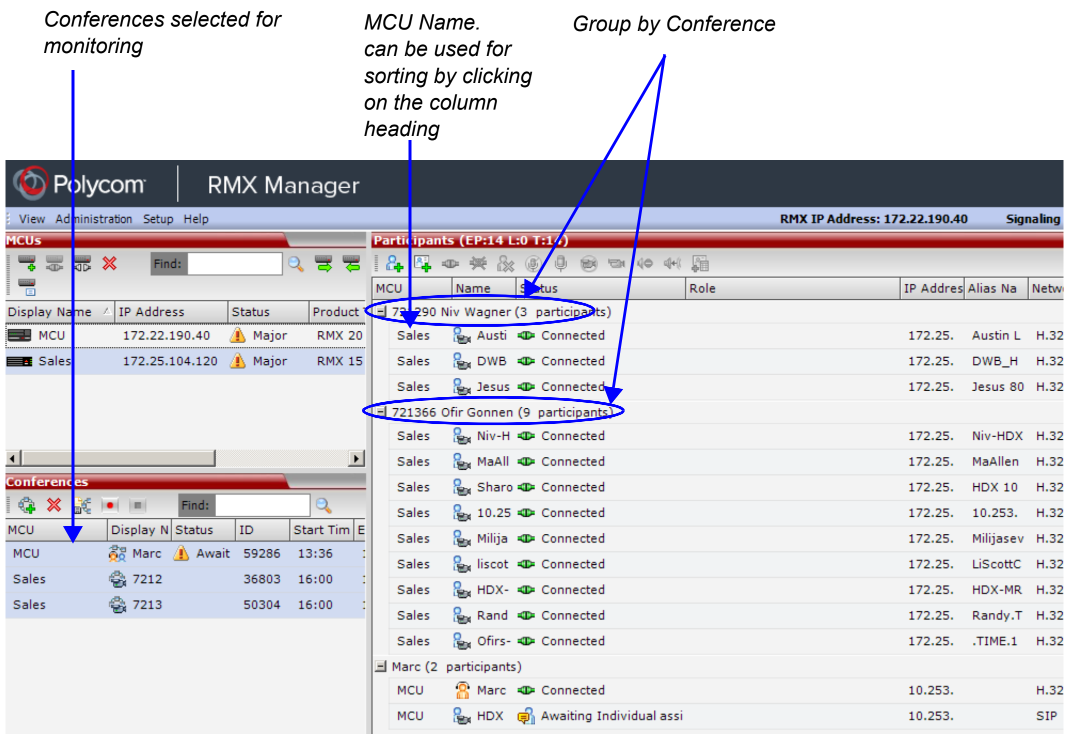
When MCUs are connected to the *RMX Manager* they are automatically monitored, that is, any ongoing conference that is started on that MCU is automatically added to the Conferences pane and its participants are monitored.

To list participants from several conferences (running on the same or different MCUs):

>> In the *Conferences* pane, using Windows multiple selection methods, select the conferences whose participants you want to list.

The participants are displayed in the *Participants* list pane.

By default, the participants are grouped by conferences, and the name of the MCU is displayed in the first column of the properties table, enabling sorting according to MCU name.

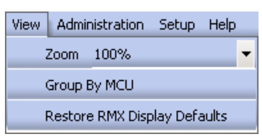


Grouping the Participants by MCU

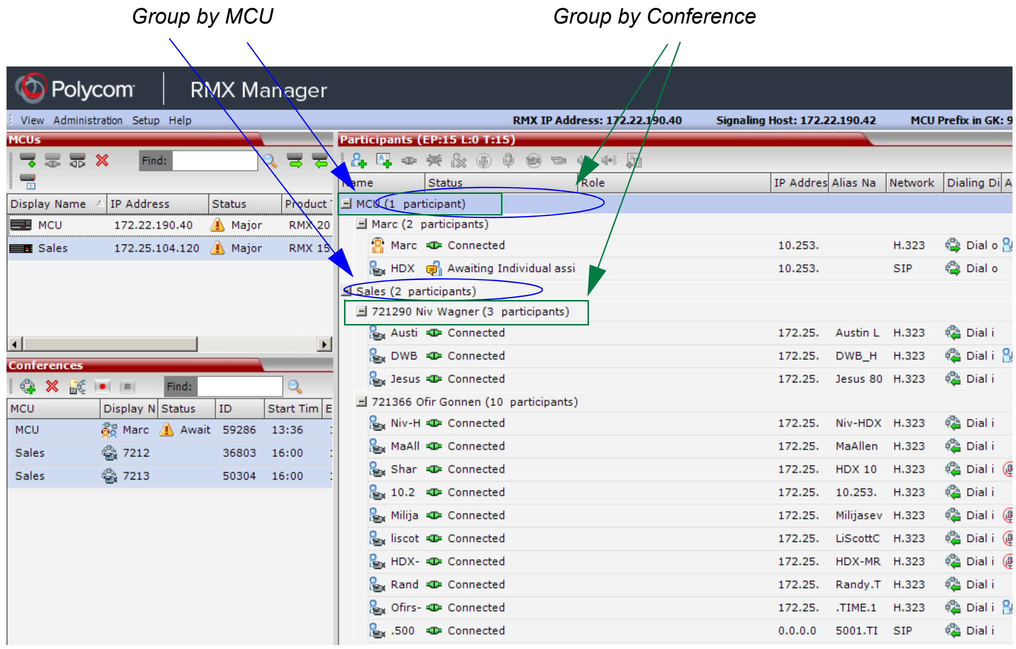
The Participants can be grouped by MCU and then by conferences.

To change the display mode for the Participants pane:

>> On the *RMX Menu*, click **View > Group by MCU**.



The *Participants* pane display changes accordingly.



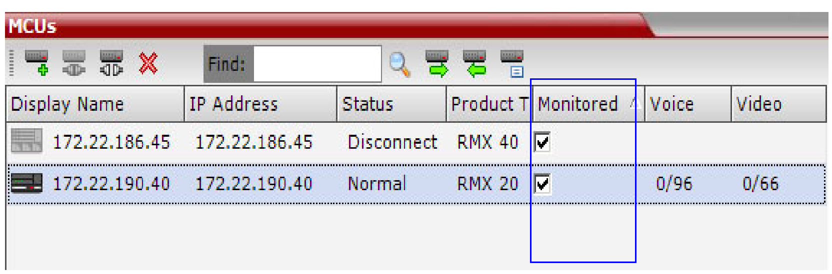
To toggle between the two display modes, click **View > Group by MCU.**

Start Monitoring/Stop Monitoring

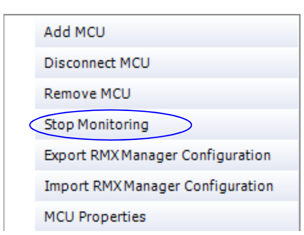
By default, all conferences running on connected RMXs are monitored.

You can stop the automatic monitoring of conferences on a specific MCU in one of the following methods:

- By clearing the check box in the *Monitored* column in the *MCUs* pane.

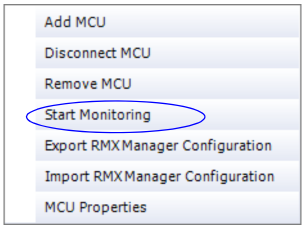


- Right-clicking the MCU icon and selecting **Stop Monitoring**.



The check box is cleared in the Monitored column.

To start monitoring again, click the check box in the *Monitored* column in the *MCUs* pane, or right-clicking the MCU icon and selecting **Start Monitoring**.



Modifying the MCU Properties

You can view the currently defined MCU settings, and modify them when required, for example, change the MCU name, IP address or Secured mode.

Use this procedure to add the *Username* and *Password* to the properties of the MCU that was automatically added to the MCU list when installing the *RMX Manager*. This enables automatic login when connecting the MCU to the *RMX Manager*.

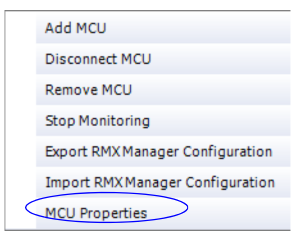
You can modify the MCU properties when the MCU is connected or disconnected.

To view and/or modify the MCU Properties:

1 Use one of the following methods:

   a Select the MCU to disconnect and click the **MCU Properties** button.

   b Right-click the MCU icon and then click **MCU Properties**.



The *MCU Properties* dialog box opens.

2 Define/modify the required parameters. For details, see *"MCU Properties"* on page 12.

3 Click **OK**.

Disconnecting an MCU

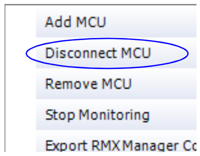
An MCU can be disconnected from the *RMX Manager*, without removing it from the *MCUs* list.

To disconnect an MCU:

1 Use one of the following methods:

   a Select the MCU to disconnect and click the **Disconnect MCU** button.

b Right-click the MCU icon and then click **Disconnect MCU**.



The MCU icon changes to disconnected and any ongoing conference running on that MCU will not be monitored in this *RMX Manager*; they are removed from the *Conferences* pane. This MCU can still be monitored and controlled by other users.

Removing an MCU from the MCUs Pane

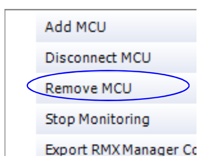
An MCU can be removed from the *RMX Manager*. This function should be used if the MCU hardware was disconnected and removed from the network.

To Remove an MCU from the list:

1 Use one of the following methods:

a Select the MCU to disconnect and click the **Delete**  button.

b Right-click the MCU icon and then click **Remove MCU**.



A confirmation message is displayed.

2 Click **OK** to confirm or **Cancel** to abort the operation.

The MCU icon is removed from the MCUs pane.

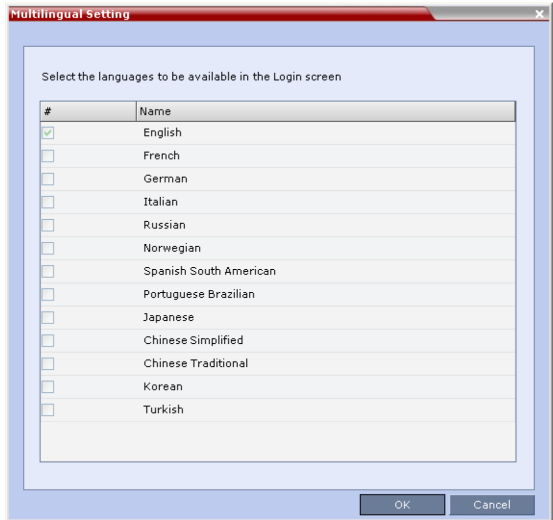
Changing the RMX Manager Language

You can change the language of the *RMX Manager* menus and dialog boxes. Only one language can be selected at a time and the *RMX Manager* application must be restarted after changing the display language.

To select a language:

1 On the *RMX Manager* menu, click **Setup > Customize Display Settings > Multilingual Settings**.

The *Multilingual Settings* dialog box opens, displaying the current language selection.



2 Click the check box of the required language. Only one language can be selected.

3 Click **OK**.

4 Restart the *RMX Manager* application to implement the language change.

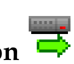
Import/Export RMX Manager Configuration

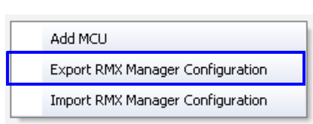
The *RMX Manager* configuration that includes the MCU list and the multilingual selection can be save to any workstation/PC on the network and imported to any *Multi-RMX Manager* installed in the network. This enables the creation of the MCUs list once and distributing it to all *RMX Manager* installations on the network.

In addition, when upgrading to a previous version, the MCU list is deleted, and can be imported after upgrade.

The exported file is save in XML format and can be edited in any text editor that can open XML files.

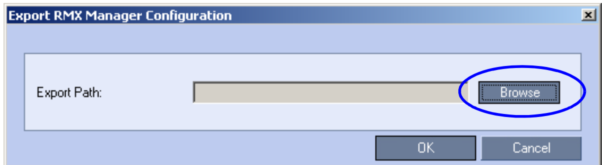
To Export the RMX Manager Configuration:

1 In the *Multi-RMX Manager*, click the **Export RMX Manager Configuration**  button in the toolbar, or right-click anywhere in the MCUs pane and then click **Export RMX Manager Configuration**.



The *Export RMX Manager Configuration* dialog box opens.

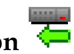
2 Click the **Browse** button to select the location of the save file, or enter the required path in the *Export Path* box.

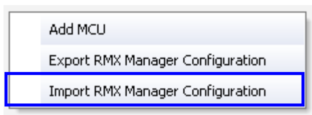


The selected file path is displayed in the *Export Path* box.

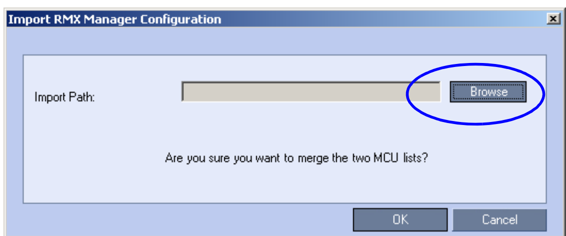
3 Click **OK** to export the *RMX Manager* configuration.

To Import the RMX Manager Configuration:

1 In the *Multi-RMX Manager*, click the **Import RMX Manager Configuration**  button in the toolbar, or right-click anywhere in the MCUs pane and then click **Import RMX Manager Configuration**.

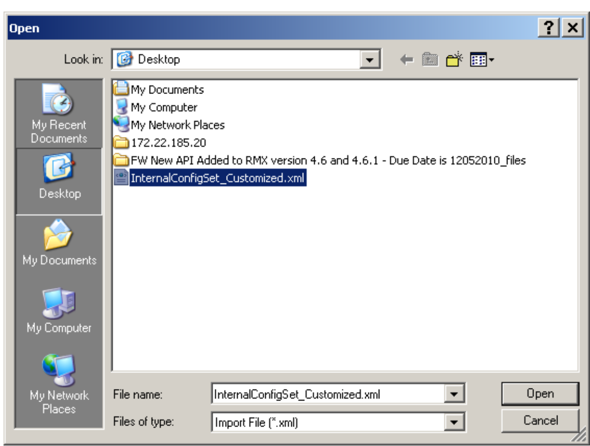


The *Import RMX Manager Configuration* dialog box opens.



2 Click the **Browse** button to select the saved file, or enter the required path in the *Export Path* box.

The *Open* dialog box is displayed.



3 Select the XML file previously saved, and click the **Open** button.

The selected file path is displayed in the *Import Path* box.

4 Click **OK** to import the file.

Installing RMX Manager for Secure Communication Mode

The *RMX Manager* cannot be downloaded from a site, operating in *Secure Communication Mode*, without a valid TLS certificate.

The following procedure describes how to obtain a TLS certificate and download the *RMX Manager* from a site operating in *Secure Communication Mode*.

> FIPS is always enabled in *Ultra Secure Mode*, and when ClickOnce is used to install *RMX Manager*, the workstation must have one of the following installed:
>
> - *.NET Framework 3.5* or a later version of the *.NET Framework*.
> - *.NET Framework 2.0* plus *Service Pack 1* or later.

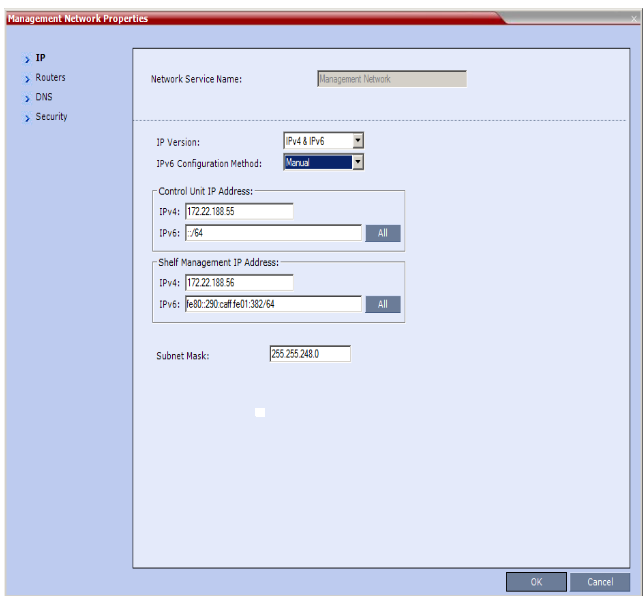
To install the RMX Manager:

1 Set the RMX to *Non Secure Communication Mode*

a In the *RMX Management* pane, click **IP Network Services.**

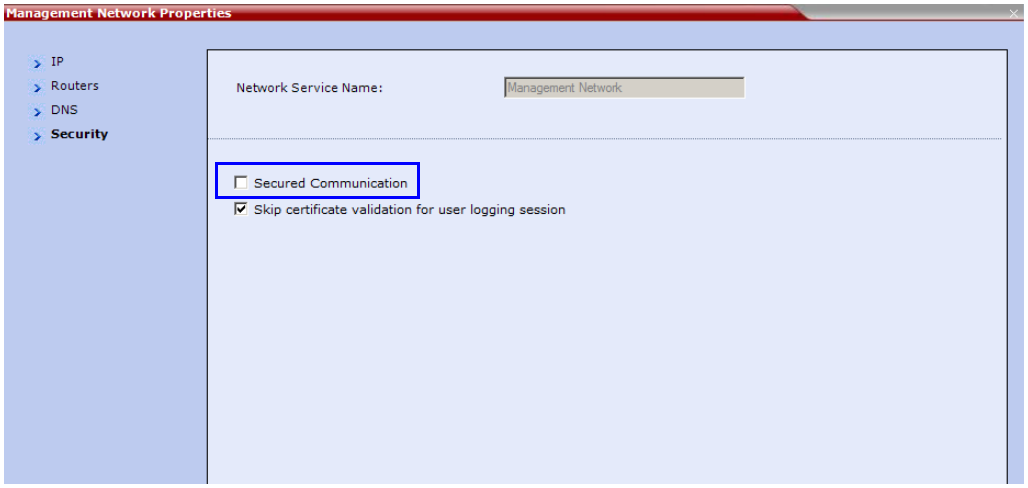
b In the *IP Network Services* list pane, double click the **Management Network** entry.

The *Management Network Properties* dialog box is displayed.



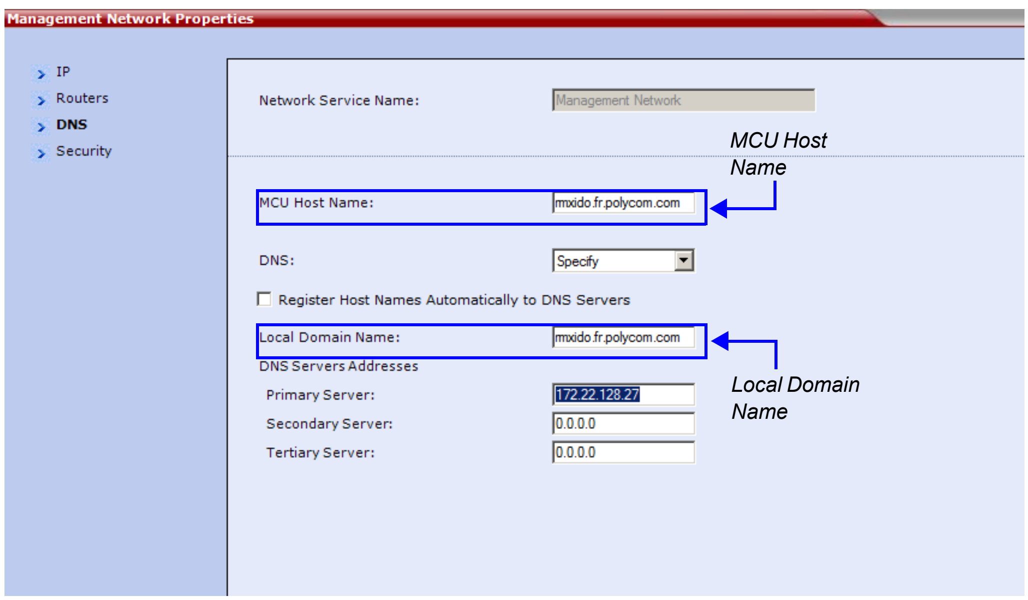
c Click on the *Security* tab.

The *Security* tab is displayed.



d Clear the *Secured Communication* check box.

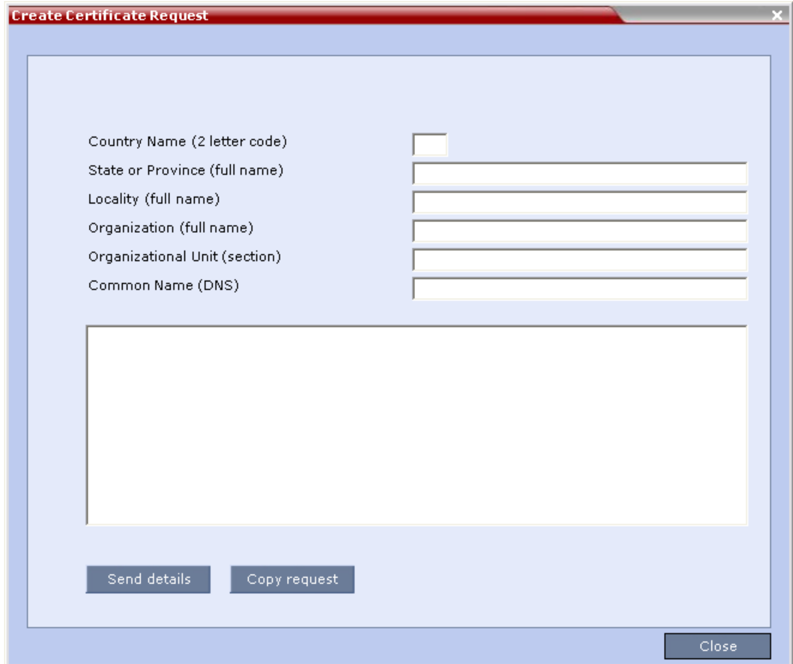
2 Click the **DNS** tab.



3 Enter the *Local Domain Name*.

The *Local Domain Name* must be the same as the *MCU Host Name*. If the content of these two fields are not identical an active alarm is created.

4 Create a *Certificate Request*.



For more information, see "*Purchasing a Certificate"* on page **F-2**.

Certificates can also be created and issued using an *Internal Certificate Authority*. For more information see "*Using an Internal Certificate Authority"* on page **20-27**.

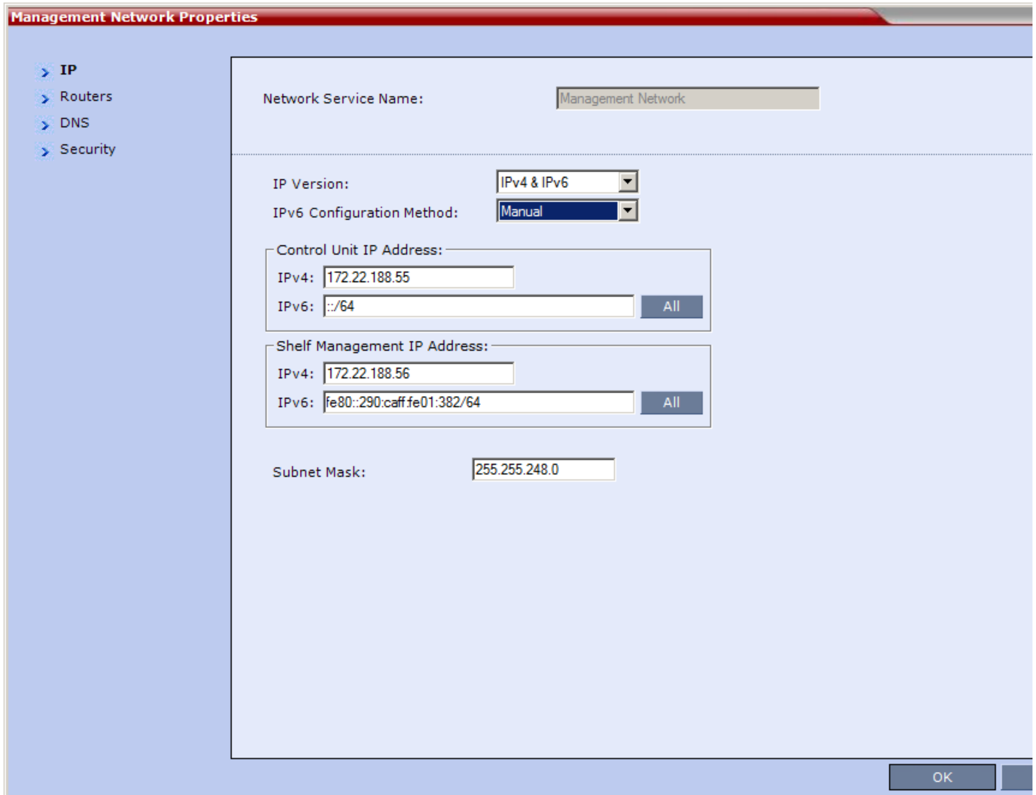
5 Install the certificate.

For more information, see *Appendix F*, "*Installing the Certificate"* on page **F-4**.

6 Set the RMX to *Secure Communication Mode*

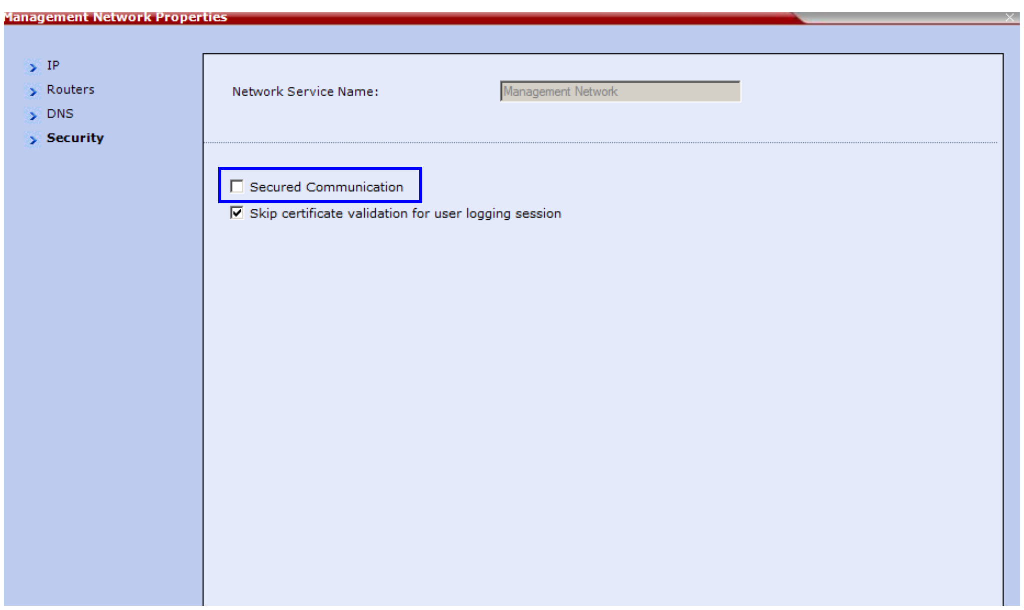
- **a** In the *RMX Management* pane, click **IP Network Services.**
- **b** In the *IP Network Services* list pane, double click the **Management Network** entry.

The *Management Network Properties* dialog box is displayed.



c Click on the *Security* tab.

The *Security* tab is displayed.



d Select the *Secured Communication* check box.

e Click **OK**.

7 Reset the RMX:

- **a** In the *RMX Management* pane, click the **Hardware Monitor button**.

  The *Hardware Monitor* pane is displayed.

- **b** Click the **Reset** ( ) button.

8 Install the *RMX Manager*. For more information see "*Installing the RMX Manager"* on page 20-2.

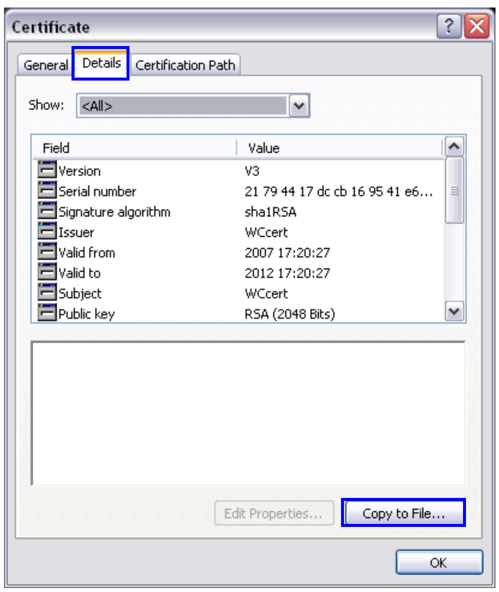
Using an Internal Certificate Authority

If your TLS certificate was created and issued by an *Internal Certificate Authority*, it may not be seen as having been issued by a trusted *Certificate Authority*. The *RMX Manager* is not downloaded successfully and a warning is received stating that the certificate was not issued by a trusted *Certificate Authority*.

To add the Internal Certificate Authority as a trusted Certificate Authority:

1 Navigate to the folder where the certificate (.cer) file is saved.

2 Open the certificate file.



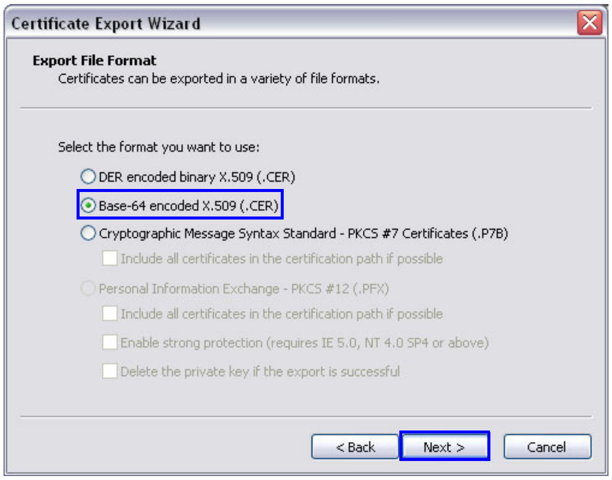
3 Click the **Detail** tab.

4 Click the **Copy to File** button.

The *Certificate Export Wizard* is displayed.

5 Click the **Next** button.

The *Export File Format* dialog box is displayed.



6 Select **Base-64 encoded X.509 (.CER)**.

7 Click the **Next** button.

The *File to Export* dialog box is displayed.

8 In the *File Name* field, enter the file name for the exported certificate.

9 Click the **Next** button.

The final *Certificate Export Wizard* dialog box is displayed.

10 Click the **Finish** button.

The successful export message is displayed.

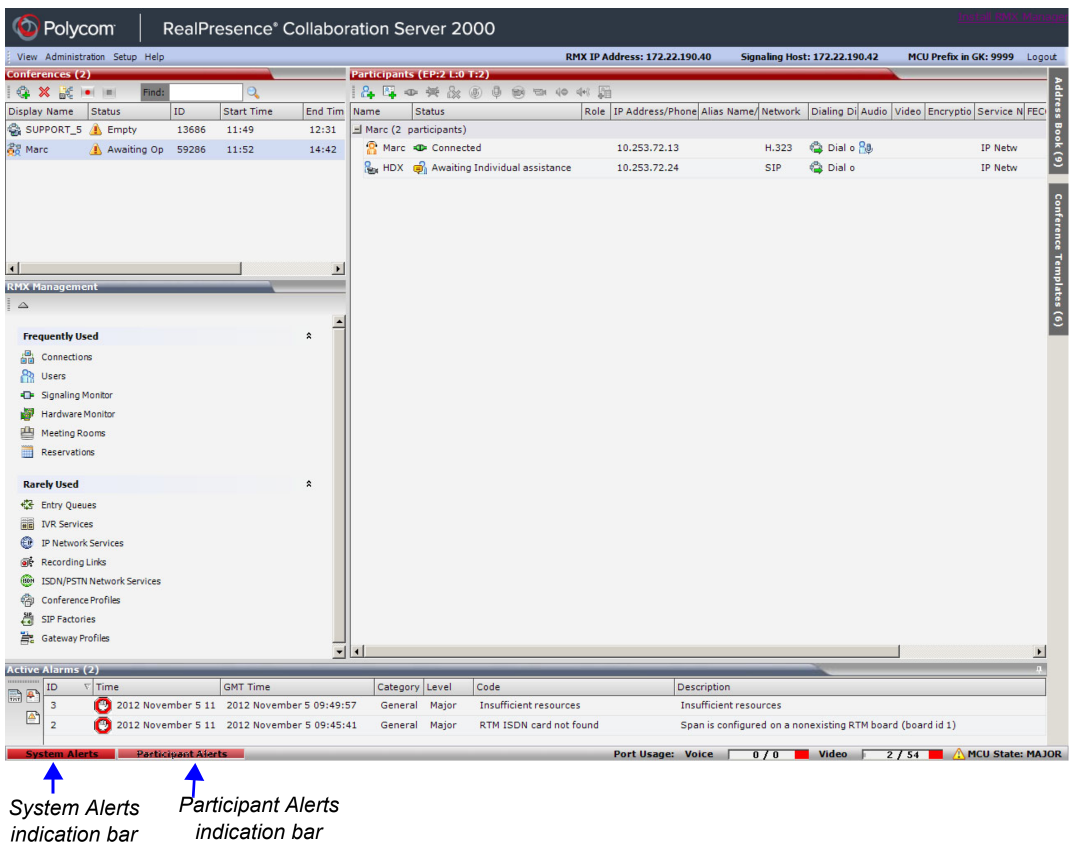
11 Click the **OK** button.

21

RealPresence Collaboration Server (RMX) Administration and Utilities

System and Participant Alerts

The MCU alerts users to any faults or errors the MCU encountered during operation. Two indication bars labeled *System Alerts* and *Participant Alerts* signal users of system errors by blinking red in the event of an alert.



The *System Alerts* indication bar blinks red prompting the user to view the active alarms. Once viewed, the *System Alerts* indication bar becomes statically red until the errors have been resolved in the MCU.

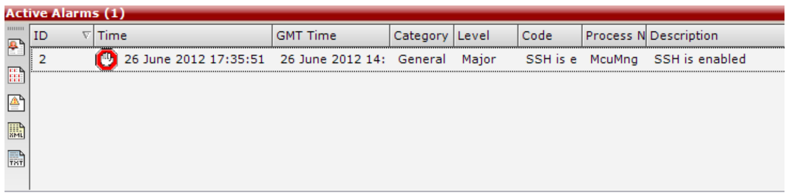
The *Participants Alerts* indication bar blinks red indicating participant connection difficulties in conferences. Once viewed, the *Participant Alerts* indication bar becomes statically red until the errors have been resolved in the MCU.

System Alerts

System Alerts are activated when the system encounters errors such as a general or card error. The system errors are recorded by the RMX and can be generated into a report that can be saved in *.txt format.

To view the System Alerts list:

1 Click the red blinking **System Alerts** indication bar.
The *Active Alarms* pane opens. This screen indicates what events have not been resolved.



The following columns appear in the *Active Alarms* pane:

***Table 21-1** Active Alarms Pane Columns*

Field	Description
ID	An identifying number assigned to the system alert.
Time	Lists the local date and time that the error occurred. This column also includes the icon indicating the error level (as listed in the level column).
GMT Time	Lists the date and time according to Greenwich Mean Time (GMT) that the error occurred.
Category	Lists the type of error. The following categories may be listed: • **File** – indicates a problem in one of the files stored on the MCU’s hard disk. • **Card** – indicates problems with a card. • **Exception** – indicates software errors. • **General** – indicates a general error. • **Assert** – indicates internal software errors that are reported by the software program.
Category (cont.)	• **Startup** – indicates errors that occurred during system startup. • **Unit** – indicates problems with a unit. • **MPL** - indicates an error related to a Shelf Management component (MPL component) other than an MPM, RTM or switch board.
Level	Indicates the severity of the problem, or the type of event. There are three fault level indicators:  – Major Error  – System Message  – Startup Event

Table 21-1 Active Alarms Pane Columns (Continued)

Field	Description
Code	Indicates the problem, as indicated by the error category.
Process Name	Lists the type of functional process involved.
Description	When applicable, displays a more detailed explanation of the cause of the problem.

For more information about the Active Alarms, see *Appendix B: "Alarms and Faults"* on page **B-1**.

2 Click one of the following two buttons to view its report in the *System Alerts* pane:

Active Alarms (default) – this is the default reports list that is displayed when clicking the System Alerts indication bar. It displays the current system errors and is a quick indicator of the MCU status.

Faults Full List - A list of all system faults.
Note: Viewed when logged in as a special support user.

Faults List – a list of faults that occurred previously (whether they were solved or not) for support or debugging purposes.

3 To save the *Active Alarms, Faults Full List* or *Faults* report:

— to a text file, click the **Save to Text**  button

— to an XML file, click the **Save to XML**  button

The **Save to XML** button is only available when logged in as a special support user.

The *Save* dialog window opens.

4 Select a destination folder and enter the file name.

5 Click **Save**.

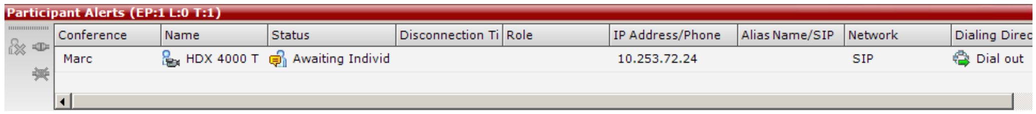
Participant Alerts

Participant Alerts enables users, participants and conferences to be prompted and currently connected. This includes all participants that are disconnected, idle, on standby or waiting for dial-in. Alerts are intended for users or administrators to quickly see all participants that need their attention.

To view the Participants Alerts list:

1 Click the red blinking **Participants Alerts** indication bar.

The *Participant Alerts* pane opens.



The *Participant Alerts* pane displays similar properties to that of the *Participant List* pane. For more information, see the *RMX 2000/4000 Getting Started Guide, "Participant Level Monitoring"* on page 3-45.

2 To resolve participant issues that created the *Participant Alerts*, the administrator can either **Connect**, **Disconnect** or **Delete** a participant.

RMX Time

To ensure accurate conference scheduling, the MCU has an internal clock that can function in standalone mode, or in synchronization with up to three *Network Time Protocol* (*NTP*) servers.

Guidelines

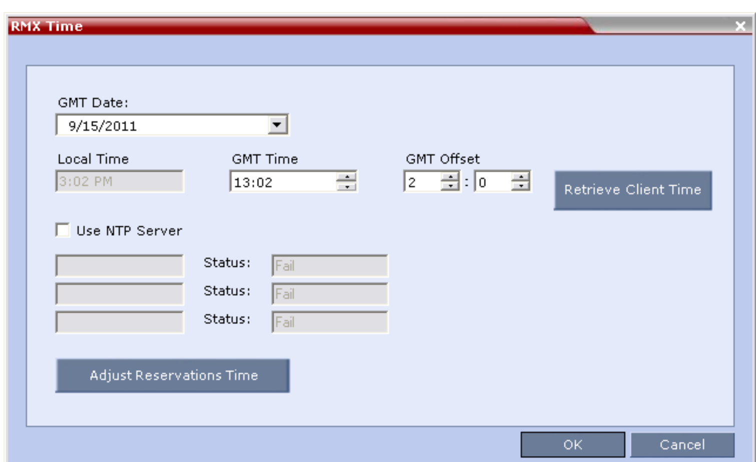
- *NTP Version 4* is the only supported protocol.
- If applicable, daylight saving adjustments must be implemented by the administrator whether the MCU is in standalone mode or synchronized with *NTP Servers*.

Altering the clock

The MCU's date and time can be set manually or enabled to synchronize with external *NTP* servers.

To Alter the MCU Time:

1 On the *RMX* menu, click **Setup > RMX Time** to open the *RMX Time* dialog box.



2 View or modify the following fields:

Table 21-2 *RMX Time – Fields Properties*

Field	Description
GMT Date	The date at Greenwich, UK.
Local Time	The MCU's local time settings, are calculated from the *GMT Time* and the *GMT Offset*.
GMT Time	The MCU's current *GMT Time* settings. Select the *Up* or *Down* arrows to alter the *GMT Time* on the MCU.
GMT Offset	The time zone difference between Greenwich and the RMX's physical location in hours and minutes. Select the *Up* or *Down* arrows to alter the *GMT Offset* time on the MCU. To enter a negative offset either type a minus in the hour box or use the down arrow and decrease the offset below zero.
Retrieve Client Time	Click this button to automatically update the MCU's *GMT Date, Time* and *Offset* to match that of the workstation.
Use NTP Server	Select this check box to synchronize the time with up to three *NTP* servers. When selected, the manual *GMT Date* and *GMT Time* setting options are disabled. The *GMT Offset* fields are still active. To implement this mode an external connection to an *NTP* server must be enabled. Enter the IP addresses of the required *NTP* servers in order of precedence. The *Status* field indicates whether registration with the *NTP Server* failed or succeeded.
Adjust Reservations Time (*Button*)	Use this button to adjust the start time of all the reservations in one operation. For more information see "*Adjusting the Start Times of all Reservations"* on page **9-16**

After resetting the MCU a delay may occur when synchronizing with the external NTP server.

Resource Management

Resource Capacity

The RealPresence Collaboration Server (RMX) 1500 supports one card type: *MPMx.*

> Three assembly variations, *MPMx-S, MPMx-D* and *MPMx-Q,* differing in resource capacity, are available for the RealPresence Collaboration Server (RMX) 1500.

The RealPresence Collaboration Server (RMX) 2000 can support three card types: *MPM, MPM+* and MPMx.

The RealPresence Collaboration Server (RMX) 4000 supports only: *MPM+* and *MPMx* cards.

> From *Version 7.1 MPM* media cards are not supported. The numbers in Table 21-3 are for *MPM* card assemblies with maximum resource capacities.

Table 21-3 summarizes the resource capacities of fully configured RMXs with the various card types per resolution in CP Conferencing mode.

> One SVC resource is equivalent to one AVC CIF resource.

Table 21-3 *Resource Capacities for Full Capacity RMX per Resolution in CP*

Resource Type	Maximum Possible Resources					
	RMX 1500	RMX 2000			RMX 4000	
	MPMx	MPM	MPM+	MPMx	MPM+	MPMx
Voice (IP)	360	400	800	720	1600	1440
Voice (PSTN)	120	400	400	400	400	400
CIF H.263	60	80	160	120	320	240
CIF H.264	90	80	160	180	320	360
CIF 60 H.264	60	–	60	120	120	240
SD30 H.264	60	20	60	120	120	240
4CIF H.263	30	20	60	60	120	120
4CIF 60 / SD 60	30	–	40	60	80	120
HD720p30	30	20	40	60	80	120
HD1080p30/HD720p60 Asymmetric	15	–	20	30	40	60
HD1080p30/HD720p60 Symmetric	15	–	–	30	–	60

Table 21-4 summarizes the resource capacities of fully configured MCUs with the various card types per line rate in VSW Conferencing mode.

Table 21-4 *Resource Capacities for Full Capacity RMX per Line Rate in VSW*

Resource Type	Maximum Possible Resources					
	RMX 1500	RMX 2000			RMX 4000	
	MPMx	MPM	MPM+	MPMx	MPM+	MPMx
Voice (IP)	360	400	800	720	1600	1440
Voice (PSTN)	120	400	400	400	400	400
VSW 2Mb	80	80	160	160	320	320
VSW 4Mb	40	40	80	80	160	160
VSW 6Mb	20	Not Applicable	40	40	80	80

- MCU's with 500MB of memory can support a maximum of 400 simultaneous participant calls, regardless of how system resources are allocated.
  MCU's with 1000MB of memory are not subject to this limitation.
- MCU memory size is listed in the *Administration* > *System Information* properties box. For more information see "*System Information"* on page **21-24**.

Resource Capacity Modes

The installed media card type (*MPM*, *MPM*+ or *MPMx)* determines the *Card Configuration Mode*, which in turn determines the resource allocation method that can be selected for the MCU. The resource allocation method determines how the system resources are allocated to the connecting endpoints and it is defined in the *Video/Voice Port Configuration*. Two allocation methods are available:

- **Flexible Resource Capacity™** – This is the default allocation mode that is used in all versions and can be used in all *Card Configuration Modes* and applies to all Conferencing Modes (SVC and AVC conferencing). The resources are only set to audio and video as a pool and the system allocates the resources according to the connecting endpoints. This mode offers flexibility in resource allocation and is available in *MPM*, *MPM*+ and *MPMx Card Configuration Modes*.

  In *Flexible Resource Capacity* mode, in *MPM*, *MPM*+ and *MPMx Card Configuration Modes,* the maximum number of resources is based on the system license, regardless of the hardware configuration of the MCU. These resources are allocated as CIF resources by default.

  Example: If the MCU is licensed for 80 video resources, but only one *MPM* card is currently installed in the MCU, the system lets you allocate 80 ports although only 40 video resources are available for participant connection. (However, an active alarm will be added to the *Active Alarms* list indicating a resource deficiency).
- **Fixed Resource Capacity™** – This mode is applies to AVC conferencing only and the resources cannot be used for SVC conferencing. It offers precise usage of resources, allowing the administrator to set the number of resources guaranteed to each *Audio Only* and video connection type in advance. This mode is available only in *MPM*+ and *MPMx Card Configuration Modes*.

In *Fixed Resource Capacity* mode, the maximum number of resources is based on the system license and the hardware configuration of the RMX. By default, these resources are allocated as HD720p30 resources, the first time *Fixed Resource Capacity* mode is activated.

Example: If two *MPM*+ cards are installed in the MCU, providing 160 video resources, and the license was not upgraded accordingly, although the system capacity is higher, resource availability for allocation does not change and remains according to the license (80). Conversely, if two *MPM*+ cards are installed in the MCU, providing 160 video resources, and the license is for 160 video resources, and one of the *MPM*+ cards is removed, the resource availability for allocation is changed to 80.

Resource Usage

SVC Conferencing

During a *SVC* conference, each SVC-endpoint uses one video port. One SVC resource is equivalent to one AVC CIF resource. When sharing content an additional video resource is used.

AVC Conferencing - Continuous Presence

Video resources usage varies according to the video resolution used by the endpoints. The higher the video resolution (quality), the greater the amount of video resources consumed by the MCU.

Table 21-5 shows the number of video resources used for each resolution.

Table 21-5 *AVC Video Resource Usage vs. Resolution (MPM, MPM+, MPMx)*

Resolution/fps	Video Resources Used		
	MPM	MPM+	MPMx
CIF/30	1	1	1 (H.264)/ 1.5 (H.261/H.263)
QCIF/30			
SIF/30			
WCIF/25	2	2.66	2
WSIF/30			
432X336/30			
SD/15			
WSD/15			
4CIF/15	2	2.66	3 (H.263 only)

Table 21-5 *AVC Video Resource Usage vs. Resolution (MPM, MPM+, MPMx) (Continued)*

<table>
<tr><th rowspan="2">Resolution/fps</th><th colspan="3">Video Resources Used</th></tr>
<tr><th>MPM</th><th>MPM+</th><th>MPMx</th></tr>
<tr><td>WSD/30</td><td rowspan="9">4</td><td rowspan="8">2.66</td><td rowspan="7">1.5</td></tr>
<tr><td>4CIF/30</td></tr>
<tr><td>4SIF/30</td></tr>
<tr><td>WVGA/30</td></tr>
<tr><td>WVGA/25</td></tr>
<tr><td>480X352/30</td></tr>
<tr><td>SD/30</td></tr>
<tr><td>WSD/60</td><td rowspan="2">3</td></tr>
<tr><td>HD720p/30</td><td>4</td></tr>
<tr><td>CIF/60</td><td rowspan="13">Not Supported</td><td rowspan="6">2.66</td><td rowspan="6">1.5</td></tr>
<tr><td>SIF/60</td></tr>
<tr><td>WSIF/60</td></tr>
<tr><td>WCIF/60</td></tr>
<tr><td>432X336/60</td></tr>
<tr><td>480X352/60</td></tr>
<tr><td>WSD/50</td><td rowspan="5">4</td><td rowspan="5">3</td></tr>
<tr><td>4CIF/50</td></tr>
<tr><td>4SIF/60</td></tr>
<tr><td>WVGA/60</td></tr>
<tr><td>WVGA/50</td></tr>
<tr><td>HD720p/60</td><td rowspan="2">8</td><td rowspan="2">6</td></tr>
<tr><td>HD1080p/30</td></tr>
</table>

AVC Conferencing - Video Switching

During a *Video Switching* conference, each endpoint uses one video (CIF) port.

AVC Conferencing - Voice

One *Audio Only* resource is used to connect a single voice participant when CIF resources have been converted to *Audio Only*. However, if no CIF resources were converted, Audio Only endpoints use one CIF video resource per connection.

When video ports are fully used, the system cannot use free audio ports for video. When audio port resources are fully used, video ports can be used, using one video port to connect one voice participant.

Video/Voice Port Configuration

The *Video/Voice Port Configuration* enables you to configure the resources per resource type and if in *MPM+* or *MPMx System Card Configuration Mode,* select the Resource Capacity Mode.

> To enable SVC-based conferencing, use the Flexible Resource Capacity Mode. SVC-based conferencing is not supported with Fixed Resource Capacity

Flexible Resource Capacity Mode

All resources are initially allocated as CIF video ports as it is a resolution commonly supported by all endpoints.

The administrator can allocate some or all of these resources as *Voice* resources and let the system allocate the remaining *Video* resources automatically as participants connect to conferences. The number of resources automatically allocated by the system resources per endpoint is according to the participant's endpoint type, capabilities and line rate.

> If the system runs out of voice ports, voice endpoints cannot connect to available video ports. Conversely, video endpoints cannot connect to available voice ports.

Flexible Resource Capacity mode is available and is the default selection in both *MPM, MPM+* and *MPMx System Card Configuration Modes.* It is the only allocation method in *MPM System Card Configuration Mode*.

Fixed Resource Capacity

Fixed Resource Capacity enables the administrator to configure in advance the maximum number of resources available for participant connections per video resolution and *Audio Only* connections. In *Fixed Resource Capacity* mode, the system is always in a known state, and when used in conjunction with the *Resource Report,* it gives the administrator precise control over resource allocation and optimization. *Fixed Resource Capacity* mode is available only in *MPM+* and *MPMx System Card Configuration Modes.*

If all resources configured to a specific video resolution are in use and an endpoint tries to connect to the MCU with that resolution, the MCU first attempts to connect the endpoint using resources of the next highest resolution level. If no resources are available at that level, the MCU tries to connect the endpoint using resources of progressively decreasing resolutions.

Example: In a system that has 10 SD ports allocated and in use, If another SD endpoint (11th) attempts to connect, the system first tries to allocate resources to the SD endpoint first from HD720 and then from HD1080 resources.

If HD resources are allocated to an SD endpoint, HD endpoints may experience a resource deficiency when trying to connect and may not be connected at HD resolution.

If there are no available HD resources the system tries to allocate resources to the SD endpoint from any available CIF resources.

If there are no available CIF resources the system tries to allocate resources to the SD endpoint from any available *Audio Only* resources. If *Audio Only* resources are allocated the HD endpoint, the participant receives an "*Audio Only*" message from the *Conference/Entry Queue IVR Service* and is connected as an *Audio Only* participant.

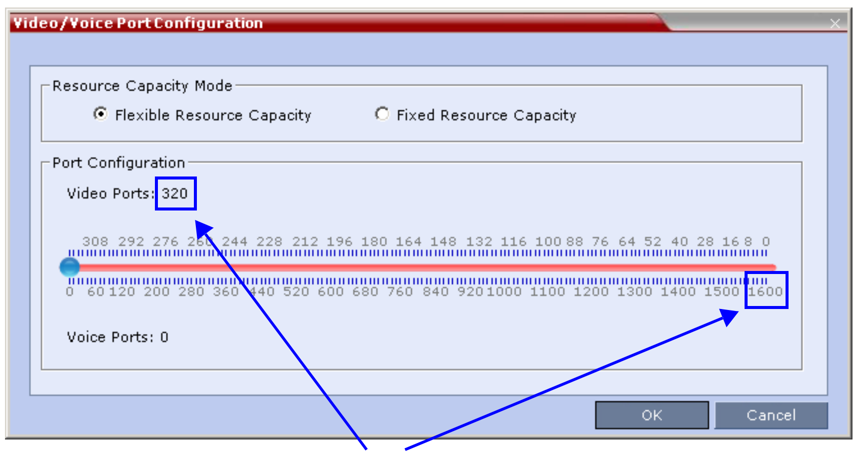
Configuring the Video/Voice Resources in MPM Mode

- Resource re-configuration should only be performed when no conferences are running on the MCU.
- Updating the configuration sequentially requires a 10 seconds wait between updates, to let the system complete the update process.

From *Version 7.1 MPM* media cards are not supported.

To allocate Voice resources:

1 In the RMX menu, click **Setup > Video/Voice Port Configuration**.
The *Video/Voice Port Configuration* dialog box opens.



Resource Maximum from License

A single slider is displayed, calibrated according to licensed video resources indicated in CIF ports in the MCU.

2 Move the slider to the number of *Voice* ports to be allocated.

The slider moves in multiples of two (in *MPM* and *MPM+ Card configuration Modes)* or three (in *MPMx Card Configuration Mode)*, converting CIF video ports to voice ports in groups of two/three, with each CIF video port converting to five voice ports in *MPM* and *MPM+ Card configuration Modes* and four voice ports in *MPMx Card Configuration Mode*. The minimum number of voice ports that can be allocated is 10 (2 video ports x 5 voice ports per video port) in *MPM* and *MPM+ Card configuration Modes* and 12 (3 video ports x 4 voice ports per video port) in *MPMx Card configuration Mode*.

3 Click **OK**.

Configuring the Video/Voice Resources in MPM+ and MPMx Mode

- Resource re-configuration should only be performed when no conferences are running on the MCU.
- Updating the configuration sequentially requires a 10 seconds wait between updates, to let the system complete the update process.

There are two *Resource Capacity* modes in *MPM+* and *MPMx Mode*:

- Flexible Resource Capacity
- Fixed Resource Capacity

Flexible Resource Capacity

Flexible Resource Capacity is the default resource allocation mode in *MPM+* and *MPMx Mode* and is functionally identical to the *MPM Flexible Resource Capacity* described above.

> On the RMX1500 MPMx-Q assembly, the use of HD with Continuous Presence requires an additional license. In the Resource Report and Resolution Configuration panes, HD settings are displayed but are not enabled and if HD is selected the system will enable SD by default.

To allocate Audio Only ports in MPM+ and *MPMx* mode:

1 **Optional** *(otherwise skip to step 2)***:** If the MCU is in *Fixed Resource Capacity* mode:

   a In the RMX menu, click **Setup > Video/Voice Port Configuration**.
   The *Video/Voice Port Configuration* dialog box opens.

   b In the *Resource Capacity Mode* box, select **Flexible Resource Capacity**.

   c Click **OK**.

2 In the RMX menu, click **Setup > Video/Voice Port Configuration**.
The *Video/Voice Port Configuration* dialog box opens.

If switching from *Fixed* mode, all video resources are allocated as CIF video ports.

3 Continue with **Step 2** of the *MPM Mode Flexible Resource Capacity* procedure described above.

Fixed Resource Capacity (for AVC-based Conferencing)

To allocate resources in Fixed Resource Capacity mode:

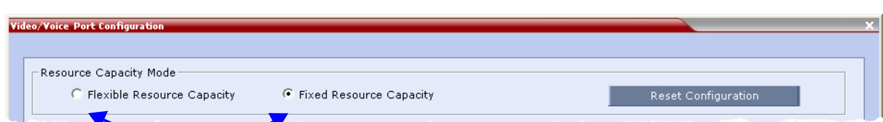
> Resource re-configuration (if the system is already set to Fixed Resource Capacity mode) should only be performed when no conferences are running on the MCU.

1 **Optional** *(otherwise skip to step 2)***:** If the MCU is not in *Fixed Capacity Mode.*

   a In the MCU menu, click **Setup > Video/Voice Port Configuration**.

   The *Video/Voice Port Configuration* dialog box opens.

   b In the *Resource Capacity Mode* box, click **Fixed**.

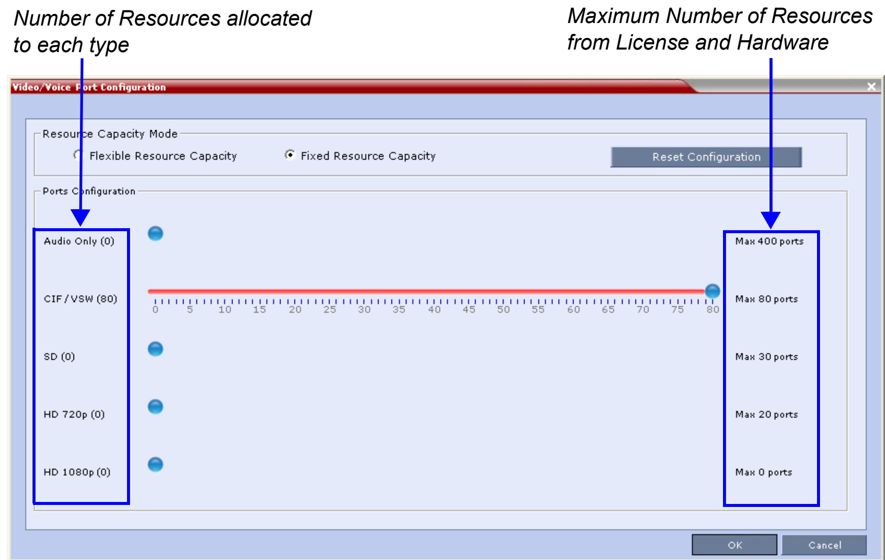


Capacity Mode Radio Buttons

   c Click **OK**.

2 In the RMX menu, click **Setup > Video/Voice Port Configuration**.

The *Video/Voice Port Configuration* dialog box opens.



On the RMX1500 MPMx-Q assembly, the use of HD with Continuous Presence requires an additional license. In the Resource Report and Resolution Configuration panes, HD settings are displayed but are not enabled and if HD is selected the system will enable SD by default.

Fixed Resource Capacity mode displays five sliders, one for each resource type: *Audio Only*, *CIF*, *SD*, *HD 720p 30fps*, *HD 1080p / HD 720p 60fps* (*HD 1080p / HD 720p 60fps* resources are represented on the same slider) where each type requires different number of video resources (in CIF ports) for connecting endpoints.

— The first time the *Fixed Resource Capacity* is selected, all resources are allocated to HD720p30 by default.

— If the allocation mode was previously *Fixed* or if it was *Auto* but *Fixed* had been selected in the past, the previous resource allocations in the mode are displayed.

The maximum number of allocatable resources of each type per fully licenced MCU with either *MPM+* or *MPMx* cards is described in Table 21-3, "*Resource Capacities for Full Capacity RMX per Resolution in CP,*" on page **21-6**. The *Max Resolution* setting of the *Resolution Configuration* dialog box does not affect resource allocation.

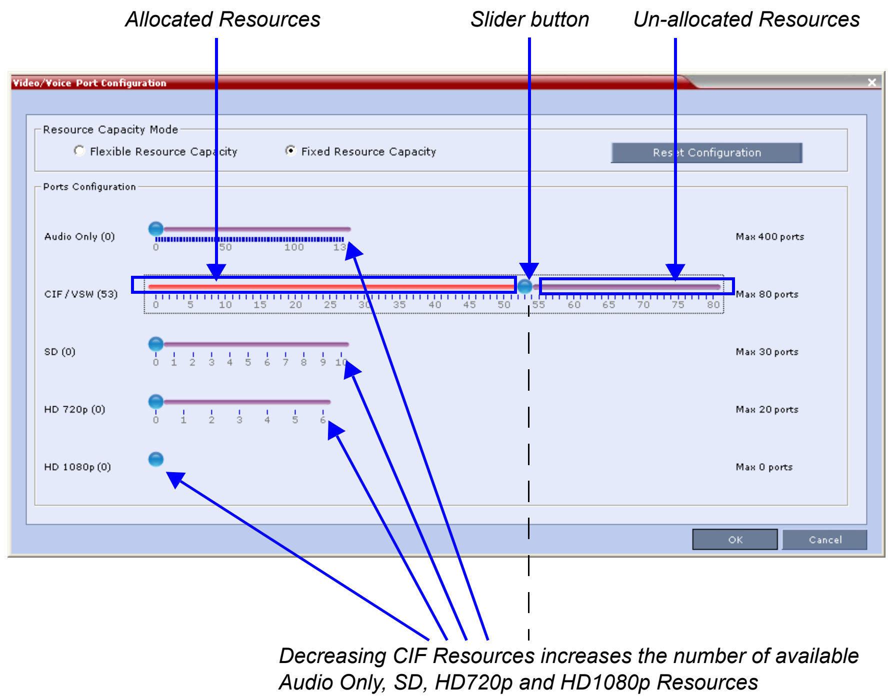
Example: If it is set to *SD30*, the *HD 1080p* slider is still displayed and *HD 1080* resources can be allocated. However, *HD 1080* participants will connect at *SD30* resolution.

Using the sliders, the administrator can manually allocate resources to the various types of video resolutions and *Audio Only* connections that can be used by connecting endpoints.

3 Move the blue slider buttons to allocate resources.

As all the resources are allocated when the dialog box opens, you must first free resources of one type by moving the blue slider button to the left, and then move blue slider button of the required resource type to the number of resources to be allocated.

On the slider bars, red areas to the left of the blue slider buttons indicate allocated resources and purple areas to the right of the blue slider buttons indicate unallocated resources in the system.



When the position of a slider is changed the system calculates the effect on the remaining system resources and adjusts the slider scales accordingly.

For example: Decreasing the allocated CIF ports from 80 to 53, free ports for allocation that can be used to allocate up to 135 voice ports or 10 SD ports or 6 HD 720p ports, or any combination of the resource types.

Allocating five *Audio Only* ports decreases the number of *CIF* ports while allocating one *SD* port decreases the number of *CIF* ports.

4 Click **OK** to activate the new *Resource Capacity*.

If after resources are recalculated there are purple areas to the right of the blue slider buttons indicating unallocated resources in the system, the system issues a warning stating that there are un-allocated resources in the system.

5 **Optional.** Repeat this procedure from **Step 2** to further optimize the resource allocation.

Un-allocated resources cannot be used by any participants.

If after recalculating the resources the system determines that there are insufficient resources to support the configuration indicated by the sliders:

— A major *System Alert* is raised with *Insufficient resources* in its *Description* field.

— The *Fixed Resource Capacity* blue slider buttons are disabled.

— A warning message is displayed.

- Click **OK** to close the warning message box.

a Optional.

- Click the **Reset Configuration** button to set all the blue slider buttons to zero.

- Reconfigure the resource allocation.
- Click **OK** to activate the new resource allocation.

b **Optional.** Click the **Cancel** button to accept the resource allocation.

The *System Alert* remains active.

Forcing Video Resource Allocation to CIF Resolution

You can set the MCU to allocate one CIF video resource to an endpoint, regardless of the resolution determined by the Conference Profile parameters. This forcing saves resources and enables more endpoints to connect to conferences.

The forcing is done by modifying the system configuration and it applies to all conferences running on the MCU.

You can specify the endpoint types for which resource allocation can be forced to CIF resource, enabling other types of endpoints to use higher resolutions in the same conference. For example, you can force the system to allocate one CIF video resource to CMAD and VSX endpoints while HDX endpoints can connect using SD or HD video resources.

Once the endpoint connects to the conference, its type is identified by the RMX and, if applicable, the RMX will connect it using one CIF resource, even if a higher resolution can be used.

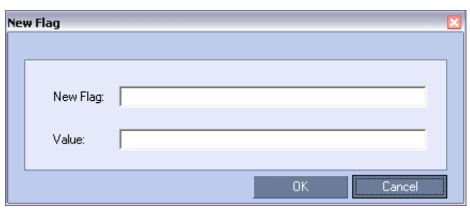
To force CIF resource:

1 On the RMX menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.

2 In the *MCMS_PARAMETERS* tab, click the **New Flag** button.

The *New Flag* dialog box is displayed.



3 In the *New Flag* field enter the flag name: **FORCE_CIF_PORT_ALLOCATION**

4 In the *Value* field enter the product type to which the CIF resource should be allocated. Possible values are:

— **CMA Desktop** for CMA desktop client

— **VSX nnnn** where nnnn represents the model number for example, VSX 8000.

You can define several endpoint types, listing them one after the other separated by semicolon (;).
For example, CMA Desktop;VSX 8000.

5 Click **OK**.
The new flag is added to the flags list.

Reset the MCU for changes to take effect. For more details, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Resetting the RMX"* on page 21-69.

To cancel the forcing of CIF resource:

1 On the RMX menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.

2 In the *MCMS_PARAMETERS* tab, double-click or select the flag **FORCE_CIF_PORT_ALLOCATION** and click the **Edit Flag** button.

3 In the *New Value* field, clear the value entries.

4 Click **OK**.

Reset the MCU for changes to take effect. For more details, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, *"Resetting the RMX"* on page 21-69

Resource Report

The *Resource Report* displays the real time resource usage according to the selected *Resource Capacity Mode*:

- *Flexible Resource Capacity Mode* available in *MPM, MPM+* and *MPMx Modes.*
- *Fixed Resource Capacity Mode* available only in *MPM+* and *MPMx Modes*

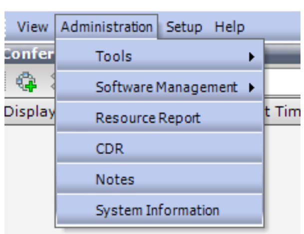
On the RMX1500 MPMx-Q assembly, the use of HD with Continuous Presence requires an additional license. In the Resource Report and Resolution Configuration panes, HD settings are displayed but are not enabled and if HD is selected the system will enable SD by default.

The *Resource Report* also includes a graphic representation of the resource usage. One resource report is available for all resource usage including SVC-based endpoints.

When the MCU is working in *MPM+* or *MPMx Mode* with *Fixed Resource Capacity Mode™* selected, additional system resources information is displayed.

Displaying the Resource Report

1 In the main toolbar, click **Administration > Resource Report**.



The *Resource Report* dialog box is displayed, showing the resource usage according to the *Resource Capacity Mode*. For each resource type, the Resource Report includes the following columns:

Table 21-6 Resource Report Fields Parameters

Column	Description
Type	The type of audio/video resources available. This applies to both AVC and SVC-based endpoints (and resources).
Total	The *Total* column displays the total number of resources of that type as configured in the system (*Occupied* and *Free*). This number reflects the current audio/video port configuration (for AVC and SVC-based conferencing). Any changes to the resource allocation will affect the resource usage displayed in the Resource Report.

Table 21-6 *Resource Report Fields Parameters (Continued)*

Column	Description
Occupied	The number of MCU resources that are used by connected AVC and SVC-based participants or reserved for defined participants.
Free	The number of MCU resources available for connecting AVC and SVC-based endpoints.

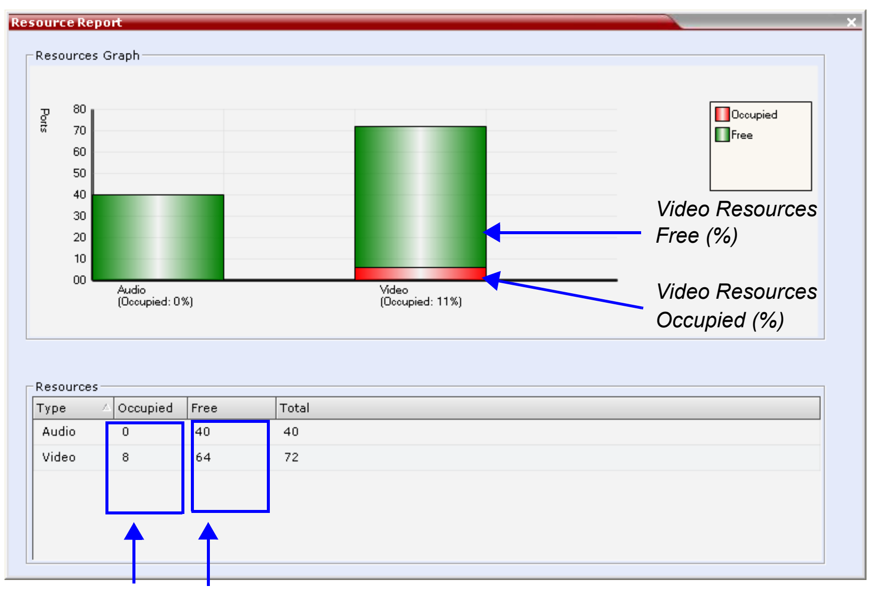
Resource Report Display in Flexible Resource Capacity Mode™

The *Resource Report* details the current availability and usage of the system resources for both AVC and SVC-based endpoint, displaying the number of free and occupied audio and video resources. A *Resources Graph* is displayed in addition to the *Resources* table.

Example: A RealPresence Collaboration Server (RMX) 2000 in ***MPM+*** *Card Configuration Mode* and *Flexible Resource Capacity Mode* has:

- 80 licensed *CIF* resources.
- 8 of its 80 *CIF* resources allocated as *Audio* = 40 *Audio* resources (8x5).
- All 40 *Audio* resources free (green).
- The remaining 72 *CIF* resources allocated as *Video* resources.
- 8 of the 72 *CIF* resources are occupied (red) while the remaining 64 are free.

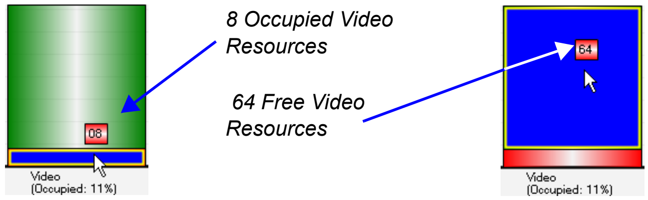
The *Resource Report* is displayed as follows:



Actual Number of Occupied and Free Audio and Video Resources

In *Flexible Resource Capacity Mode,* resource usage is displayed for *Voice* and Video resources only, where the number of video resources is represented in the equivalent of CIF resources. The number represents a pool of both AVC and SVC resources. They are displayed as percentages of the total resource type.

The actual number of occupied or free resources can also be displayed by moving the cursor over the columns of the bar graph. Moving the cursor over the *Video* bar displays the following:



Port Gauges

In *Flexible Resource Capacity* mode, the *Port Gauges* in the *Status Bar* show 0 of the 40 *Audio (Voice)* resources as occupied and 8 of the 72 *Video* resources as occupied.

Resource Report in Fixed Resource Capacity Mode™ (AVC-based Conferencing)

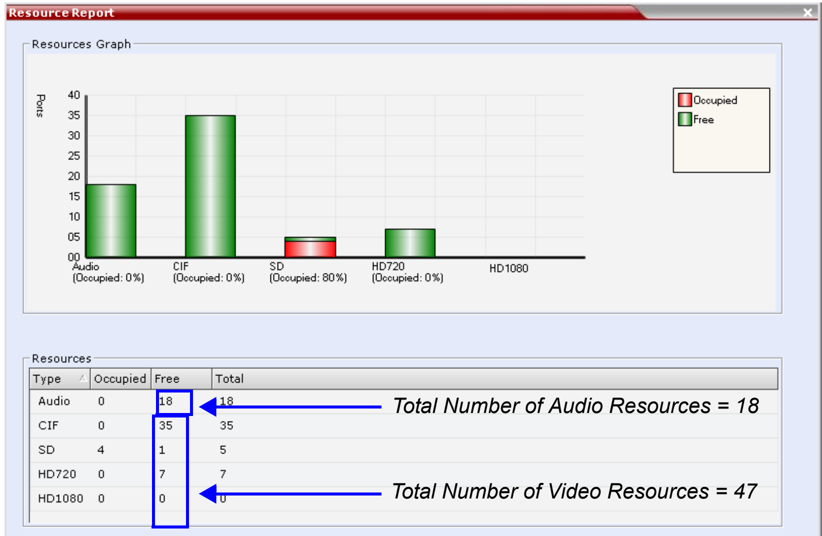
In *Fixed Resource Capacity Mode,* each resource type (*Audio, CIF, SD, HD 720p* and *HD 1080p*) is displayed as a bar of the graph, indicating the percentage of occupied and free resources for each resource type.

The data is also displayed as a *Resources* table indicating the actual number of resources occupied and free for each resource type along with a total number of each resource type.

Example: A RealPresence Collaboration Server (RMX) 2000 in ***MPM+*** *Card Configuration Mode* and *Fixed Resource Capacity Mode* has:

- 80 licensed *CIF* resources.
- 18 *Audio* resources allocated, all free (green).
- 35 *CIF* resources allocated, all free.
- 5 *SD* resources allocated, 4 occupied (red), 1 free.
- 7 *HD 720* resources allocated, all free.
- 0 *HD 1080* resources allocated.

The *Resource Report* is displayed as follows:



The actual number of occupied or free resources can also be displayed by moving the cursor over the columns of the bar graph (as explained above for *Flexible Resource Capacity*).

Port Gauges

Audio (*Voice*) resources are as displayed as in previous versions while all *Video* resource types are shown as a single group of *Video* resources.

The gauges show 0 of the 18 *Audio (Voice)* resources as occupied. The 4 occupied *SD* resources are shown as 4 occupied resources out of the total of 47 *Video* resources.

ISDN/PSTN

The *RMX 1500* supports one *ISDN* card with *4 E1/T1 PRI* lines.

On the *RMX 2000/4000* a maximum of two *RTM ISDN* cards are supported, each providing connection for up to either 7 *E1* or 9 *T1 PRI* lines.

On *RMX 1500/2000/4000*, *E1* and *T1* connections cannot be used simultaneously.

Table 21-7 lists the *ISDN* supported bit rates and their respective participant connection capacities per *RTM ISDN* card:

Table 21-7 *ISDN – E1/T1 Connection Capacity vs. Bit rate*

Bit Rates (Kbps) (Bonded)	Number of Participants per RTM ISDN Card		
	E1	T1	
128	40	40	If the conference bit rate is 128Kbps, participants connecting at bit rates lower than 128Kbps are disconnected. If the conference bit rate is above 128Kbps but does not match any of the bonded bit rates, participants are connected at the highest bonded bit rate that is less than the conference bit rate. For example: If the conference bit rate is 1024Kbps, the participant is connected at 768Kbps.
192	40	40	
256	40	40	
320	40	40	
384	34	34	
512	25	25	
768	17	17	
1152	11	11	
1472	9	9	
1536	8	8	
1920	7	6	

RMX Resource Management by CMA and DMA

When both *CMA* and *DMA* are part of the solution, following a request by the *CMA* and *DMA*, the *RMX* will send updates on resource usage to both *CMA* and *DMA,* with each application updating its own resource usage for the *RMX*. This provides better management of the RMX resources by *CMA* and *DMA*.

Guidelines

- Resource usage updates from *RMX* to the *CMA* and *DMA* are supported only with *RMX*s with *MPM*+ or *MPMx* cards.
- Both *Flexible Resource Capacity*™ and *Fixed Resource Capacity*™ modes are supported with DMA.
- Only *Flexible Resource Capacity*™ mode is supported with CMA.
- Following requests sent by *CMA* and *DMA*, the *RMX* will send the number of occupied resources for a conference or total for the MCU, according the *Resource Capacity Mode* used by the system.

— In *Flexible Resource Capacity Mode*, *CMA/DMA* receive information about how many *Video* (*CIF*) and *Audio* resources are occupied per conference or MCU according the request type sent by the *CMA* and *DMA*.

— In *Fixed Resource Capacity™ Mode*, *DMA* receives information about the number of occupied resources per resource type (Audio Only, CIF, SD, HD 720p, HD 1080p) and per conference or MCU according the request type sent by the *DMA*.

- Occupied resources are resources that are connected to ongoing conferences. Disconnected endpoints in an ongoing conference are not counted as occupied resources.
- An ongoing conference that does not include participants and the *Send Content to Legacy Endpoints* option is disabled does not occupy resources. If the *Send Content to Legacy Endpoints* option is enabled, the conference occupies one SD resource.
- The *RMX* is unaware of the resource usage split between the *CMA* and *DMA*.

Port Usage Threshold

The RMX can be set to alert the administrator to potential port capacity shortages. A capacity usage threshold can be set as a percentage of the total number of licensed ports in the system.

When the threshold is exceeded, a *System Alert* is generated.

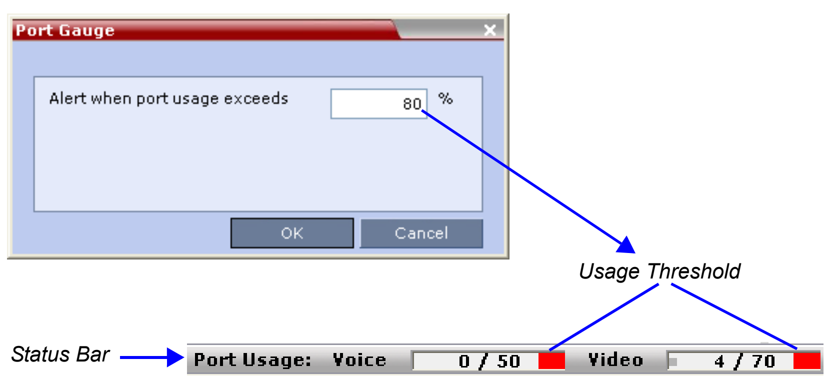
The default port capacity usage threshold is 80%.

The administrator can monitor the MCU's port capacity usage via the *Port Gauges* in the *Status Bar* of the *RMX Web Client*.

Setting the Port Usage Threshold

To Set the Port Usage Threshold:

1 In the *Setup* menu, click **Port Gauge** to open the *Port Gauge* dialog box.



2 Enter the value for the percentage capacity usage threshold.
The value is applied to the Audio and video resources according to the Video/Voice Port Configuration.

The high Port Usage threshold represents a percentage of the total number of video or voice ports available. It is set to indicate when resource usage is approaching its maximum, resulting in no free resources to run additional conferences. When port usage reaches or exceeds the threshold, the red area of the gauge flashes. The default port usage threshold is 80%.

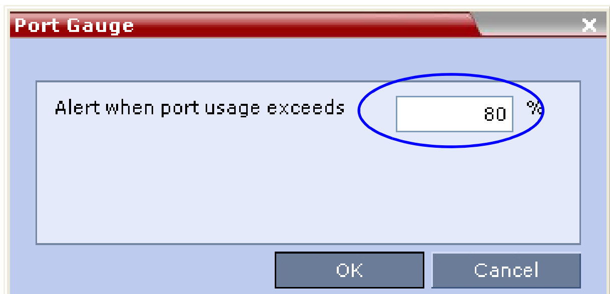
3 Click **OK.**

SIP Dial-in Busy Notification

When the system flag SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD is set to YES (NO is the default), it enables the RMX to send a busy notification to a SIP audio endpoint or a SIP device when dialing in to the RMX whose audio resource usage exceeded the Port Usage threshold.

The RMX will send a SIP busy response to SIP audio endpoints when:

- The system flag SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD is set to YES (NO is the default)
- The port usage threshold for Audio resources is exceeded. The threshold is defined in the **Setup > Port Gauge** dialog box.



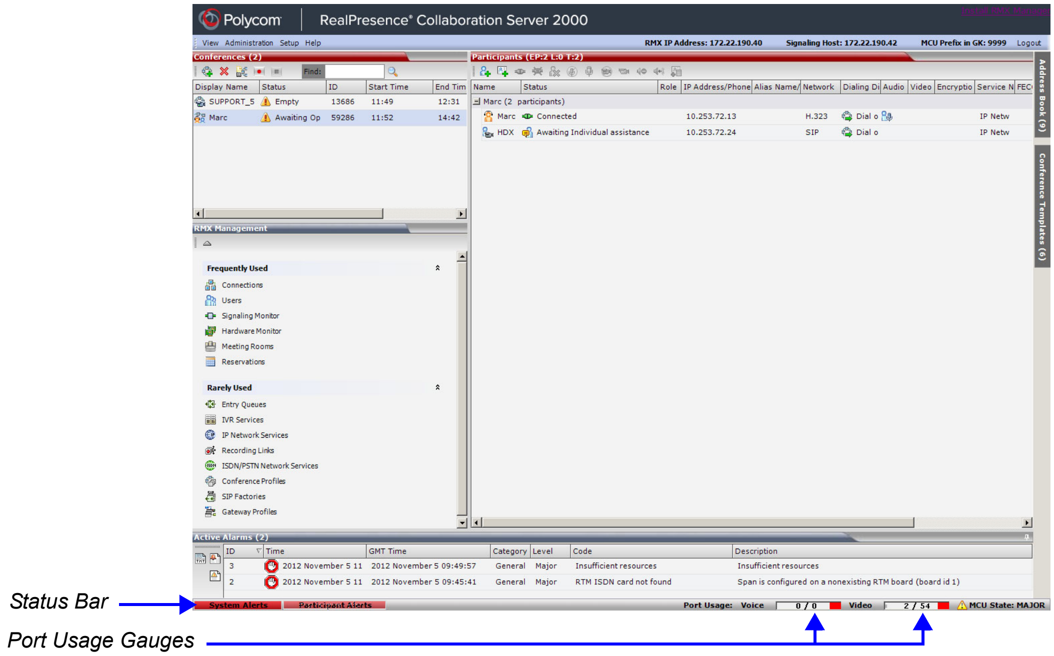
When the flag is set to YES, the system will allow SIP audio endpoints to connect to the MCU until the Port Usage threshold is reached. Once this threshold is exceeded, the SIP audio endpoints will not be able to connect, ensuring that the remaining system resources can be used by all other connections, including SIP video, H.323 cascaded links and ISDN video. When the call is rejected by the MCU because of lack of resources, the appropriate indication will be sent by the MCU to the SIP audio endpoint.

For example, if the *Port Gauge* threshold is set to 80%, when 80% of the **Audio resources** are used, the system will not allow additional SIP audio endpoints to connect and will send a busy notification to the endpoint.

This does not affect the video resources usage.

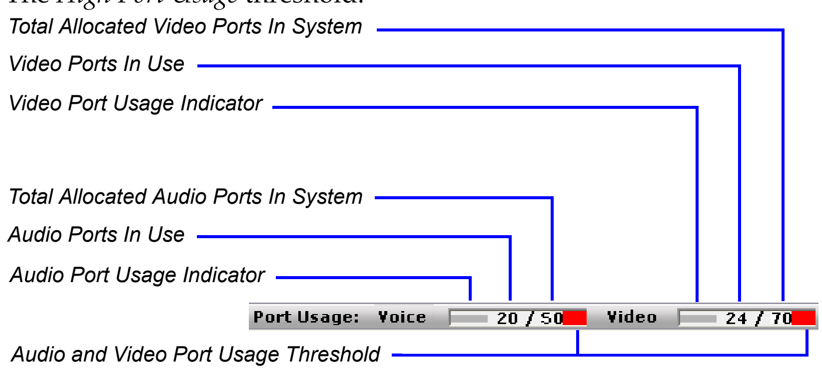
Port Usage Gauges

The *Port Usage Gauges* are displayed in the *Status Bar* at the bottom of the *RMX Web Client* screen.



The *Port Usage* gauges indicate:

- The total number of *Video* or *Voice* ports in the system according to the *Video/Voice Port Configuration*. The *Audio* gauge is displayed only if *Audio* ports were allocated by the administrator, otherwise only the *Video* port gauge is displayed.
- The number of *Video* and *Voice* ports in use.
- The *High Port Usage* threshold.



Port Gauges in Flexible/Fixed Capacity Modes

Audio Ports Gauge

- In both *Flexible* and *Fixed Capacity Modes:*
  The fraction displayed indicates the exact number of voice resources in use out of the total number of voice resources.

Video Ports Gauge

- In *Flexible Capacity Mode:*
  All video resource usage is converted to the equivalent CIF resource usage. The fraction displayed indicates the exact number of video resources in use out of the total number of video resources in the system.
- In *Fixed Capacity Mode:*
  All video ports are treated as a single group of *Video* resources regardless of their differing consumption of CIF video resources. The fraction displayed indicates the number of video resources in use out of the total number video resources in the system.

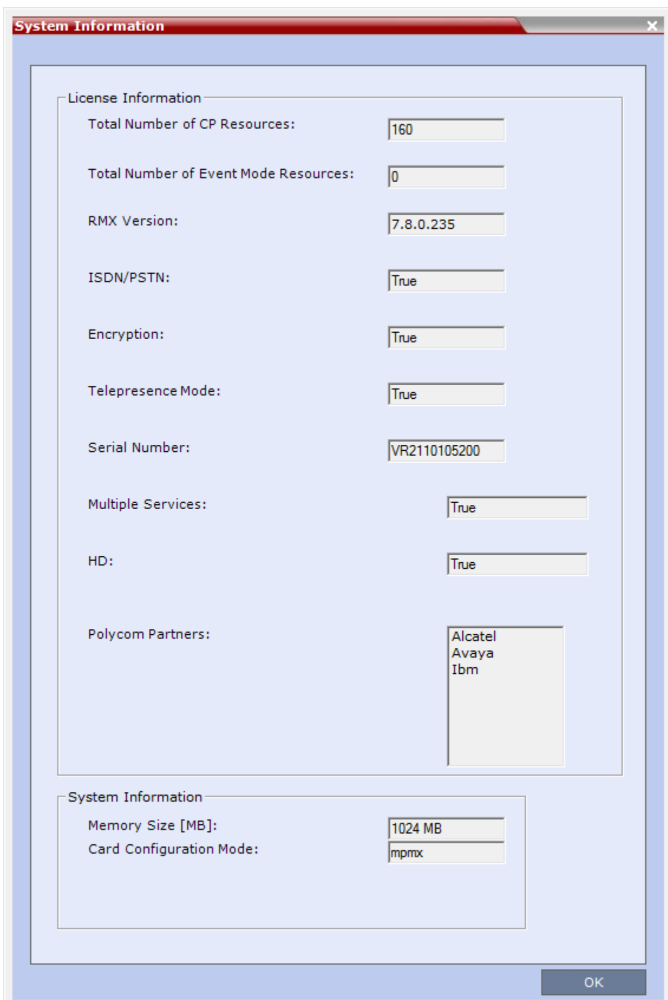
System Information

System Information includes *License Information*, and general system information, such as system memory size and *Media Card Configuration Mode*.

To view the System Information properties box:

>> On the RMX menu, click **Administration > System Information**.

The *System Information* properties box is displayed.



The *System Information* properties box displays the following information:

Table 21-8 *System Information*

Field	Description
Total Number of CP Resources	Displays the number of video participants licensed for the system. Each CP resource represents one CIF video resource. Each SVC resource is equivalent to one CIF video resource.
Total Number of Event Mode Resources	Displays the number of video/voice participants licensed for a system in Event Mode Licensing. It also determines the conference type that is available on the system. 0 - indicates that this Licensing mode is disabled for this system.
RMX Version	Displays the *System Software Version* of the RMX.
ISDN/PSTN	Indicates whether RTM ISDN hardware has been detected in the system and if ISDN/PSTN is included in the MCU license. Range: True / False
Encryption	Indicates whether *Encryption* is included in the MCU license. Encryption is not available in all countries. Range: True / False
Telepresence Mode	The field value indicates whether the system is licensed to work with *RPX* and *TPX Telepresence* room systems. Range: True / False
Serial Number	Displays the *Serial Number* of the RMX.
Multiple Services	A *Multiple Services* license is installed.
HD	Only for *RMX1500* with a *MPMx-Q* media card. Indicates if the MCU is licensed to connect endpoints at *HD* resolutions in *Continuous Presence* conferences.
Polycom Partners	Indicates that the *System Software* contains features for the support of specific *Polycom Partner* environments.
Memory Size [MB]	Indicates the RMX system memory size in MBytes. Possible values: • 1024 MB – *Version 7.1* and later requires 1024 or memory. • 500 MB – If Memory size is 512MB, *Version 7.1 and later* are not supported. DO NOT upgrade the system to *Version 7.1 and later*.

***Table 21-8** System Information (Continued)*

Field	Description
Card Configuration Mode	Indicates the MCU configuration as derived from the installed media cards: • **MPM:** Only MPM cards are supported. MPM+ and MPMx cards in the system are disabled. It is the mode used in previous RMX versions. From Version 7.1, MPM media cards are not supported. • **MPM+:** Only MPM+ cards are supported. MPM and MPMx cards in the system are disabled. • **MPMx:** Only MPMx cards are supported. MPM and MPM+ cards in the system are disabled. **Note:** When started with Version 7.0 installed, the RMX enters MPM+ mode by default, even if no media cards are installed: • The RMX only switches between MPM, MPM+ and MPMx *Card Configuration Modes* if MPM, MPM+ or MPMx cards are removed or swapped while it is powered on. • The *Card Configuration Mode* switch occurs during the next restart. • Installing or swapping MPM, MPM+ or MPMx cards while the system is off will not cause a mode switch when the system is restarted - it will restart in the *Card Configuration Mode* that was active previous to powering down.

- The RMX only switches between *MPM, MPM+* and *MPMx Card Configuration Modes* if *MPM / MPM+ / MPMx* cards are removed or swapped while it is running.
- The *Card Configuration Mode* switch occurs during the **next** restart.
- Installing or swapping *MPM / MPM+ / MPMx* cards while the system is off will not cause a mode switch when the system is restarted – it will restart in the *Card Configuration Mode* that was active previous to powering down.
- From *Version 7.1*, *MPM* media cards are not supported.

SNMP (Simple Network Management Protocol)

SNMP enables managing and monitoring of the MCU status by **external** managing systems, such as HP OpenView or through web applications.

The RMX's implementation of SNMPv3 is FIPS 140 compliant.

MIBs (Management Information Base)

MIBs are a collection of definitions, which define the properties of the managed object within the device to be managed. Every managed device keeps a database of values for each of the definitions written in the MIB.

The SNMP systems poll the MCU according to the MIB definitions.

Traps

The MCU is able to send Traps to different managers. Traps are messages that are sent by the MCU to the SNMP Manager when an event such as MCU Reset occurs.

Guidelines

- *Version 1*, *Version 2* and *Version 3* traps are supported.
- When *SNMPv3* is selected only *SNMPv3 Queries* and *Traps* receive responses.
- A mixture of *Version 1*, *Version 2* and *Version 3* traps is not permitted.

MIB Files

The H.341 standard defines the MIBs that H.320 and H.323 MCUs must comply with. In addition, other MIBs should also be supported, such as MIB-II and the ENTITY MIB, which are common to all network entities.

The MIBs are contained in files in the *SNMP MIBS* sub-directory of the RMX root directory. The files should be loaded to the SNMP external system and compiled within that application. Only then can the SNMP external application perform the required monitoring tasks.

The MULTI-MEDIA_MIB_TC must be compiled before compiling the other MIBs.

Private MIBs

- *RMX-MIB (RMX-MIB.MIB)*
  - Contains the statuses of the RMX: Startup, Normal and Major.
  - Contains all the Alarms of the RMX that are sent to the SNMP Manager.

Support for MIB-II Sections

The following table details the MIB-II sections that are supported:

Table 21-9 Supported MIB-II Sections

Section	Object Identifier
system	mib-2 1

Table 21-9 Supported MIB-II Sections (Continued)

Section	Object Identifier
interfaces	mib-2 2
ip	mib-2 4

The Alarm-MIB

MIB used to send alarms. When a trap is sent, the Alarm-MIB is used to send it.

H.341-MIB (H.341 – H.323)

- Gives the address of the gatekeeper.
- Supports H.341-MIB of SNMP events of H.323.

Standard MIBs

This section describes the MIBs that are included with the RMX. These MIBs define the various parameters that can be monitored, and their acceptable values.

MIB Name	Description
MULTI-MEDIA-MIB-TC (MULTIMTC.MIB)	Defines a set of textual conventions used within the set of Multi Media MIB modules.
H.320ENTITY-MIB (H320-ENT.MIB)	This is a collection of common objects, which can be used in an H.320 terminal, an H.320 MCU and an H.320/H.323 gateway. These objects are arranged in three groups: Capability, Call Status, and H.221 Statistics.
H.320MCU-MIB (H320-MCU.MIB)	Used to identify managed objects for an H.320 MCU. It consists of four groups: System, Conference, Terminal, and Controls. The *Conference* group consists of the active conferences. The *Terminal* group is used to describe terminals in active MCU conferences. The *Controls* group enables remote management of the MCU.
H323MC-MIB (H323-MC.MIB)	Used to identify objects defined for an H.323 Multipoint Controller. It consists of six groups: System, Configuration, Conference, Statistics, Controls and Notifications. The *Conference* group is used to identify the active conferences in the MCU. The *Notifications* group allows an MCU, if enabled, to inform a remote management client of its operational status. **Note:** The RMX supports only one field in H.341-H323MC MIB. The RMX reports the Gatekeeper address using H.341-H323MC MIB – 323McConfigGatekeeperAddress (0.0.8.341.1.1.4.2.1.1.4) in response to a query from a manager.
MP-MIB (H323-MP.MIB)	Used to identify objects defined for an H.323 Multipoint Processor, and consists of two groups: Configuration and Conference. The *Configuration* group is used to identify audio/video mix configuration counts. The *Conference* group describes the audio and video multi-processing operation.

MIB Name	Description
MIB-II/RFC1213-MIB (RFC1213.MIB)	Holds basic network information and statistics about the following protocols: TCP, UDP, IP, ICMP and SNMP. In addition, it holds a table of interfaces that the Agent has. MIB-II also contains basic identification information for the system, such as, Product Name, Description, Location and Contact Person.
ENTITY-MIB (ENTITY.MIB)	Describes the unit physically: Number of slots, type of board in each slot, and number of ports in each slot.

Unified MIB

The RMX uses the Polycom Unified MIB, in addition to the RMX specific MIB. The Polycom Unified MIB is an MIB that is used by many Polycom products. The following table describes the information provided by the RMX in the Unified MIB.

Table 22 *Unified MIB SNMP Fields*

Name	Type	Description
Debug	Boolean	Indicates whether the unit is in a debugging state.
IncomingCallsReqrGK	Boolean	Indicates whether a gatekeeper is required to receive incoming H.323 calls.
OutgoingCallsReqrGK	Boolean	Indicates whether a gatekeeper is required to make outgoing H.323 calls.
HDBitrateThrshld	Integer	The minimum bit rate required by endpoints in order to connect to an HD conference.
MaxCPRstln	Integer	Maximum resolution of a CP conference.
MaxCPRstlnCfg	Integer	Configured resolution for a CP conference.
EndpointDispayName	String	The name of the MCU that is displayed on the screen of endpoints that are connecting to the conference.
PALNTSC	NTSC/PAL/ AUTO	The video encoding of the RMX.
SeparateMgmtNet	Boolean	Indicates whether management network separation is enabled.
NumPorts	Integer	Total number of ports.
NumVideoPorts	Integer	Number of ports configured for video.
ServiceH323	Integer	Indicates the status of H.323 capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
ServiceSIP	Integer	Indicates the status of SIP capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.

Table 22 *Unified MIB SNMP Fields (Continued)*

Name	Type	Description
ServiceISDN	Integer	Indicates the status of SIP capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
RsrcAllocMode	Fixed/ Flexible	The resource allocation method which determines how the system resources are allocated to the connecting endpoints.
McuSystemStatus	Integer	System State.
FanStatus	Boolean	Status of the hardware fan.
PowerSupplyStatus	Boolean	Status of the power supply.
IntegratedBoardsStatus	Boolean	Status of the integrated boards.
UltraSecureMode	Boolean	Indicates whether the RMX is operating in Ultra Secure Mode.
ChassisTemp	Integer	The temperature of the chasis.
NumPortsUsed	Integer	Number of ports currently in use.
NewCallsPerMinute	Integer	New calls in the last minute.
ScsfNewCallsPerMinute	Integer	Successful new calls in the last minute.
FldNewCallsPerMinute	Integer	Failed new calls in the last minute.
PctScsflNewCalls	Integer	Percentage of new calls in the last minute which were successful.
CallsEndedScsflPerMin	Integer	Number of calls in the last minute which ended with a success code.
CallsEndedFailedPerMin	Integer	Number of calls in the last minute which ended with a failure code.
CallsEndedScsfl	Integer	Number of calls in the last minute which ended with a success code.
CallsEndedFailed	Integer	Number of calls in the last minute which ended with a failure code.
NumActvCnfrncs	Integer	Number of active conferences.

Traps

Three types of traps are sent as follows:

1 ColdStart trap. This is a standard trap which is sent when the MCU is reset.

```
coldStart notification received from: 172.22.189.154 at 5/20/
  2007 7:03:12 PM
  Time stamp: 0 days 00h:00m:00s.00th
  Agent address: 172.22.189.154 Port: 32774 Transport: IP/UDP
  Protocol: SNMPv2c Notification
  Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
  Community: public
  Enterprise: enterprises.8072.3.2.10
  Bindings (3)
    Binding #1: sysUpTime.0 *** (timeticks) 0 days
    00h:00m:00s.00th
    Binding #2: snmpTrapOID.0 *** (oid) coldStart
```

Figure 1 *An Example of a ColdStart Trap*

2 Authentication failure trap. This is a standard trap which is sent when an unauthorized community tries to enter.

```
authentication Failure notification received from:
  172.22.189.154 at 5/20/2007 7:33:38 PM
  Time stamp: 0 days 00h:30m:27s.64th
  Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP
  Protocol: SNMPv2c Notification
  Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
  Community: public
  Enterprise: enterprises.8072.3.2.10
  Bindings (3)
    Binding #1: sysUpTime.0 *** (timeticks) 0 days
    00h:30m:27s.64th
    Binding #2: snmpTrapOID.0 *** (oid) authenticationFailure
```

Figure 2 *An Example of an Authentication Failure Trap*

3 Alarm Fault trap. The third trap type is a family of traps defined in the POLYCOM-RMX-MIB file, these traps are associated with the RMX active alarm and clearance (proprietary SNMP trap).

```
rmxFailedConfigUserListInLinuxAlarmFault notification received
  from: 172.22.189.154 at 5/20/2007 7:04:22 PM
  Time stamp: 0 days 00h:01m:11s.71th
  Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP
  Protocol: SNMPv2c Notification
  Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP
  Community: public
  Bindings (6)
    Binding #1: sysUpTime.0 *** (timeticks) 0 days
    00h:01m:11s.71th
    Binding #2: snmpTrapOID.0 *** (oid)
    rmxFailedConfigUserListInLinuxAlarmFault
    Binding #3: rmxAlarmDescription *** (octets) Insufficient
    resources
    Binding #4: rmxActiveAlarmDateAndTime *** (octets) 2007-6-
    19,16:7:15.0,0:0
    Binding #5: rmxActiveAlarmIndex *** (gauge32) 2
    Binding #6: rmxActiveAlarmListName *** (octets) Active
    Alarm Table
 *  Binding #7: rmxActiveAlarmRmxStatus *** (rmxStatus) major
```

Figure 3 An Example of an Alarm Fault Trap

Each trap is sent with a time stamp, the agent address, and the manager address.

Status Trap

The MCU sends status traps for the status **MAJOR** - a trap is sent when the card/MCU status is MAJOR.

All traps are considered "MAJOR".

Defining the SNMP Parameters in the RMX

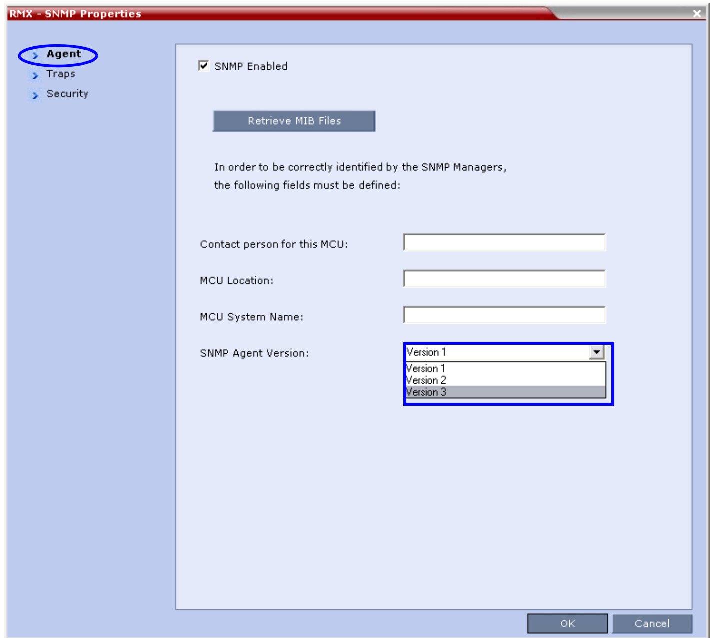
The SNMP option is enabled via the *RMX Web Client* application.

The addresses of the Managers monitoring the MCU and other security information are defined in the *RMX Web Client* application and are saved on the MCU's hard disk. Only users defined as Administrator can define or modify the SNMP security parameters in the *RMX Web Client* application.

To enable SNMP option:

1 In the *RMX Web Client* menu bar, click **Setup > SNMP**.

The *RMX-SNMP Properties - Agent* dialog box is displayed.



This dialog box is used to define the basic information for this MCU that will be used by the SNMP system to identify it.

2 In the *Agent* dialog box, click the **SNMP Enabled** check box.

3 Click the **Retrieve MIB Files** button to obtain a file that lists the MIBs that define the properties of the object being managed.

The *Retrieve MIB Files* dialog box is displayed.

4 Click the **Browse** button and navigate to the desired directory to save the MIB files.

5 Click **OK**.
The path of the selected directory is displayed in the *Retrieve MIB Files* dialog box.

6 Click the **Save** button.
The MIB files are saved to the selected directory.

7 Click **Close** to exit the *Retrieve MIB Files* dialog box.

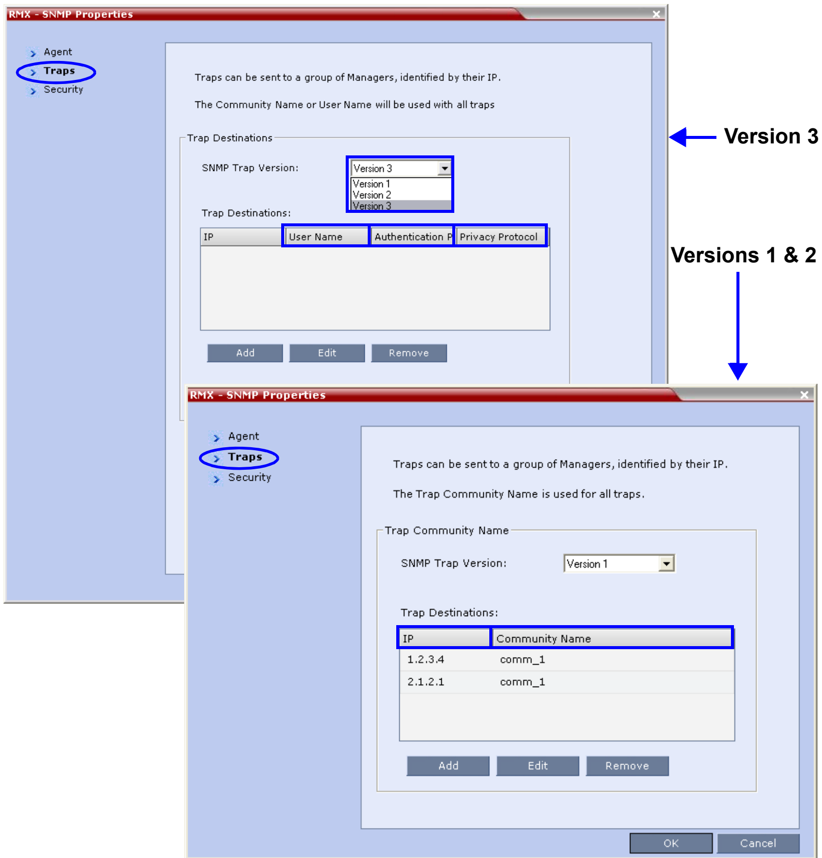
8 In the *Agent* dialog box, define the parameters that allow the SNMP Management System and its user to easily identify the MCU.

Table 21-1 *RMX-SNMP Properties - Agent Options*

Field	Description
Contact person for this MCU	Type the name of the person to be contacted in the event of problems with the MCU.
MCU Location	Type the location of the MCU (address or any description).
MCU System Name	Type the MCU's system name.

9 Click the **Traps** tab.

The *RMX-SNMP Properties – Traps* dialog box opens.



Traps are messages sent by the MCU to the SNMP Managers when events such as MCU Startup or Shutdown occur. Traps may be sent to several SNMP Managers whose IP addresses are specified in the *Trap Destinations* box.

10 Define the following parameters:

Table 21-2 *SNMPv3 - Traps*

Field	Description
SNMP Trap Version	Specifies the version, either Version 1 2 or 3 of the traps being sent to the IP Host. Polycom software supports the standard SNMP version 1 and 2 traps, which are taken from RFC 1215, convention for defining traps for use with SNMP. **Note:** The SNMP Trap Version parameters must be defined identically in the external SNMP application.

***Table 21-2** SNMPv3 - Traps (Continued)*

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td rowspan="6">Trap Destination</td><td colspan="3">This box lists the currently defined IP addresses of the Manager terminals to which the message (trap) is sent.</td></tr>
<tr><td>IP</td><td>Enter the IP address of the SNMP trap recipient.</td><td>All Versions</td></tr>
<tr><td>Community Name</td><td>Enter the Community Name of the manager terminal used to monitor the MCU activity</td><td>Version 1 and Version 2</td></tr>
<tr><td>User Name</td><td>Enter the name of the user who is to have access to the trap.</td><td rowspan="3">Version 3</td></tr>
<tr><td>Authentication Protocol</td><td>Enter the authentication protocol: MD5 or SHA.</td></tr>
<tr><td>Privacy Protocol</td><td>Enter the privacy protocol: DES or AES.</td></tr>
</table>

11 Click the **Add** button to add a new Manager terminal.

The *New Trap Destination* dialog box opens.

12 Type the **IP Address** and the **Community name** of the manager terminal used to monitor the MCU activity, and then click **OK**.

The *Community name* is a string of characters that will be added to the message that is sent to the external Manager terminals. This string is used to identify the message source by the external Manager terminal.

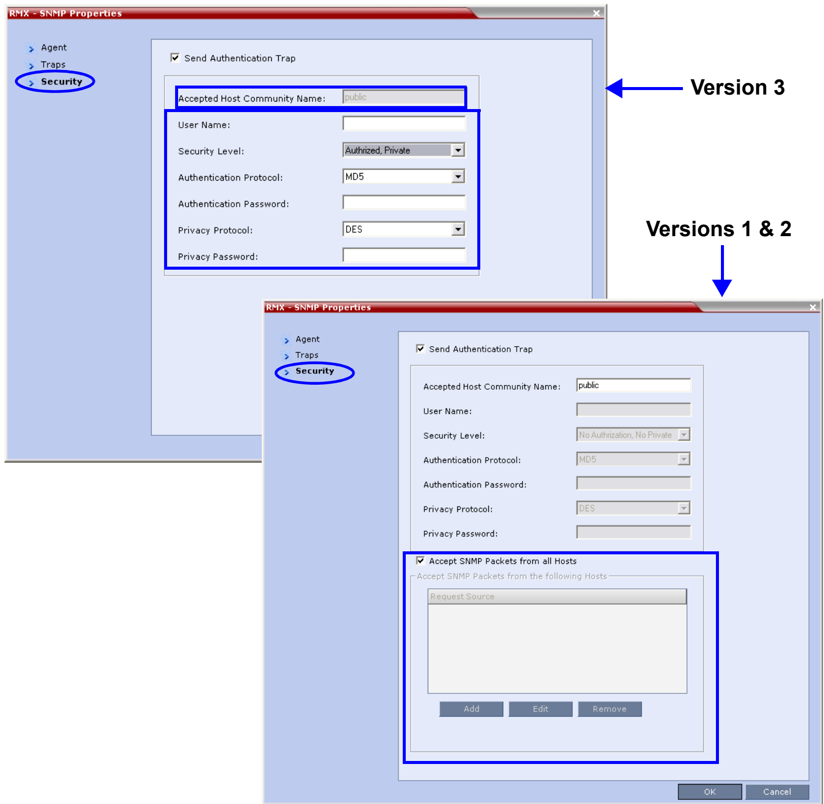
The new *IP Address* and *Community name* is added to the *Trap Destinations* box.

a To delete the IP Address of a Manager terminal, select the address that you wish to delete, and then click the **Remove** button.

The IP address in the *Trap Destinations* box is removed.

13 Click the **Security** tab.

The *RMX-SNMP Properties – Security* dialog box opens.



This dialog box is used to define whether the query sent to the MCU is sent from an authorized source. When the *“Accept SNMP packets from all Hosts”* is disabled, a valid query must contain the appropriate community string and must be sent from one of the Manager terminals whose IP address is listed in this dialog box.

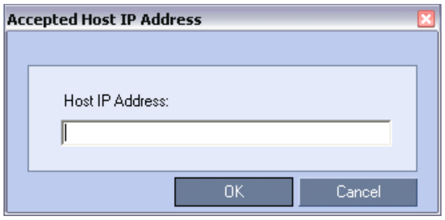
14 Define the following parameters:

Table 21-3 *SNMP - Security*

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td>Send Authentication Trap</td><td colspan="2">Select this check box to send a message to the SNMP Manager when an unauthorized query is sent to the MCU. When cleared, no indication will be sent to the SNMP Manager.</td><td rowspan="4">Versions 1 & 2</td></tr>
<tr><td>Accept Host Community Name</td><td colspan="2">Enter the string added to queries that are sent from the SNMP Manager to indicate that they were sent from an authorized source.
Note: Queries sent with different strings will be regarded as a violation of security, and, if the Send Authentication Trap check box is selected, an appropriate message will be sent to the SNMP Manager.</td></tr>
<tr><td>Accept SNMP Packets from all Host</td><td colspan="2">Select this option if a query sent from any Manager terminal is valid. When selected, the Accept SNMP Packets from These Hosts option is disabled.</td></tr>
<tr><td>Accept SNMP Packets from the following Hosts</td><td colspan="2">Lists specific Manager terminals whose queries will be considered as valid. This option is enabled when the Accept SNMP Packets from any Host option is cleared.</td></tr>
<tr><td>User Name</td><td colspan="2">Enter a User Name of up to 48 characters
Default: Empty</td><td rowspan="7">Version3</td></tr>
<tr><td>Security Level</td><td colspan="2">Select a Security Level from the drop-down menu.
Range: No Auth, No Priv; Auth, No Priv; Auth, Priv
Default: Auth, Priv</td></tr>
<tr><td>Authentication Protocol</td><td>Select the authentication protocol
Range: MD5, SHA
Default: MD5</td><td rowspan="2">These fields are enabled if Authentication is selected in the Security Level field.</td></tr>
<tr><td>Authentication Password</td><td>Enter an Authentication Password.
Range: 8 - 48 characters
Default: Empty</td></tr>
<tr><td>Privacy Protocol</td><td>Select a Privacy Protocol.
Range: DES, AES
Default: DES</td><td rowspan="3">These fields are enabled if Privacy is selected in the Security Level field.</td></tr>
<tr><td>Privacy Password</td><td>Enter a Privacy Password.
Range: 8 - 48 characters
Default: Empty</td></tr>
<tr><td>Engine ID</td><td>Enter an Engine ID to be used for both the Agent and the Trap.
Default: Empty</td></tr>
</table>

15 To specifically define one or more valid terminals, ensure that the *Accept SNMP Packets from any Host* option is cleared and then click the **Add** button.

The *Accepted Host IP Address* dialog box opens.



16 Enter the *IP Address* of the Manager terminal from which valid queries may be sent to the MCU, and then click **OK**.
Click the **Add** button to define additional *IP Addresses*.
The *IP Address* or *Addresses* are displayed in the *Accept SNMP Packets from These Hosts* box.

Queries sent from terminals not listed in the *Accept SNMP Packets from These Hosts* box are regarded as a violation of the MCU security, and if the *Send Authentication Trap* check box is selected, an appropriate message will be sent to all the terminals listed in the *SNMP Properties – Traps* dialog box.

17 In the *RMX - SNMP Properties - Security* dialog box, click **OK**.

Hot Backup

Hot Backup implements a high availability and rapid recovery solution.

Two RMX's are configured in a *Master/Slave* relationship: the *Master MCU* is active while the *Slave* acts as a passive, fully redundant *Hot Backup* of the *Master MCU*.

All conferencing activities and configuration changes that do not require a *System Reset* are mirrored on the *Slave MCU* five seconds after they occur on the *Master MCU*.

In the event of failure of the *Master MCU*, the *Slave MCU* transparently becomes active and assumes the activities and functions with the backed up settings of the failed *Master MCU*.

In ***AVC-based conferencing***, both dial-in and dial-out participants are automatically dialed out and reconnected to their conferences. However, the *Hot Backup* solution is optimized for dial-out participants as all the dial-out numbers are defined in the system and are available for redialing.

In ***SVC-based conferencing***, since dial-out is unavailable, SVC-enabled endpoints will have to manually reconnect to the conference.

The following entities are automatically backed up and updated on the *Slave MCU*:

- Ongoing Conferences
  - Layout
  - Video Force
  - Participant Status (Muted, Blocked, Suspended)
- Reservations
- Meeting Rooms
- Entry Queues
- SIP Factories

- Gateway Profiles
- IVR services (excluding .wav files)
- Recording Link
- Profiles
- IP Network Settings:
  - H.323 settings
  - SIP settings
  - DNS settings
  - Fix Ports (TCP, UDP) settings
  - QoS settings

Guidelines

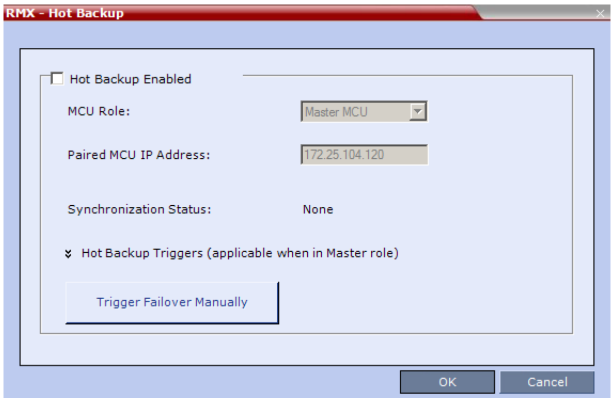
- Both *Master* and *Slave MCUs* must have the same software version installed.
- The *Users* list and *Passwords* must be the same on both the *Master* and *Slave MCUs*.
- There must be connectivity between the *Master* and *Slave* MCUs, either on the same network or on different networks connected through routers.
- In the event of failure of the *Master MCU* the *Slave MCU* assumes the role of the *Master MCU*. The *Master/Slave* relationship is reversed: the *Slave*, now active, remains the *Master* and the previous *Master MCU*, when restarted, assumes the role of *Slave MCU*.
- No changes to the *Slave MCU* are permitted while it is functioning as the *Hot Backup*. Therefore no ongoing conferences or reservations can be added manually to the *Slave* MCU.
- If *Hot Backup* is disabled, all ongoing conferences and *Reservations* backed up on the *Slave MCU* are automatically deleted.
- In *Hot Backup* configuration, the *SIP* and *H.323 Authentication* configuration of the User Name and Password in the *IP Network Service Properties - Security* tab of the *Master* RMX are not backed up in the *Slave* RMX.
- *Master* and *Slave* initial roles can be reversed only after all ongoing conferences and *Reservations* are deleted.
- Changes to the *Master MCU* that require a *System Reset* can only be made after *Hot Backup* is disabled.
- *Video/Voice Port Configurations* on the Master MCU are not synchronized with the Slave MCU. You must manually set the Video/Voice Port Configurations on both the Master and Slave MCUs to the same level.

Enabling Hot Backup

To enable Hot Backup:

1 On the RMX menu, click **Setup > Hot Backup**.

The *RMX Hot Backup* dialog box is displayed.



2 Complete or modify the following fields:

Table 21-4 *Hot Backup*

Field	Description
Hot Backup Enabled	Select this check box to enable *Hot Backup*.
MCU Role:	This setting determines the role of the MCU in the *Hot Backup* configuration. Select either **Master MCU** or **Slave MCU** from the drop-down menu.
Paired MCU IP Address	Enter the *Control Unit IP Address* of the: • *Slave MCU* (if this MCU is the *Master*) • *Master MCU* (if this MCU is the *Slave*)
Synchronization Status	The status of the synchronization between the Master and Slave MCUs in the *Hot Backup* configuration is indicated as: • **OK** - Hot Backup is functioning normally, and the Master and Slave MCUs are synchronized. • **Attempting** - *Hot Backup* is attempting to synchronize the Master and Slave MCUs. • **Fail** - A failure occurred while trying to synchronize the paired MCUs. • **None** - *Hot Backup* has not been enabled.

3 Click **OK**.

Using Hot Backup Triggers

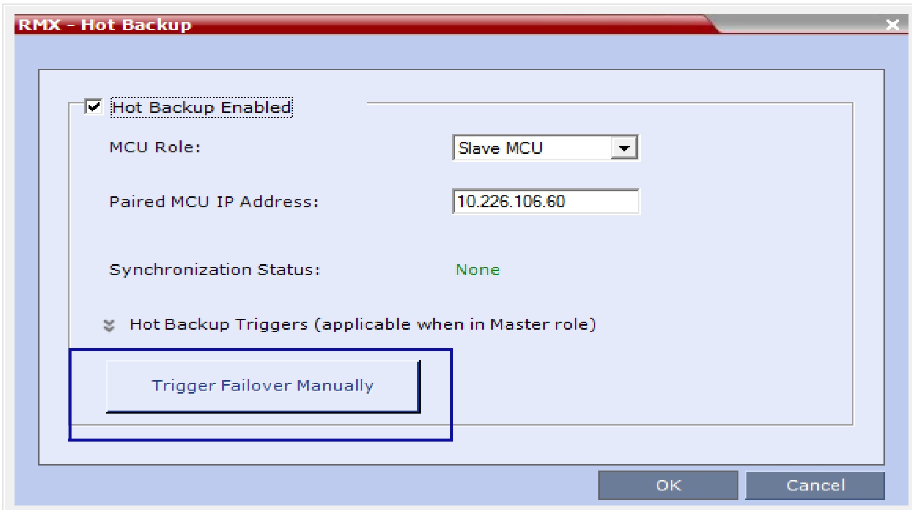
Hot Backup is initiated by the slave MCU on detection of no response from the master MCU on a "Keep Alive" operation. The *Hot Backup* triggers initiates the *Hot Backup* swap from Master to Slave when the selected conditions on the Master MCU occur.

Guidelines

- *Hot Backup* triggers should be configured on both the Master and Slave MCUs.
- *Hot Backup* triggers are not synchronized between the Master and Slave MCUs.

Configuring the Hot Backup Triggers

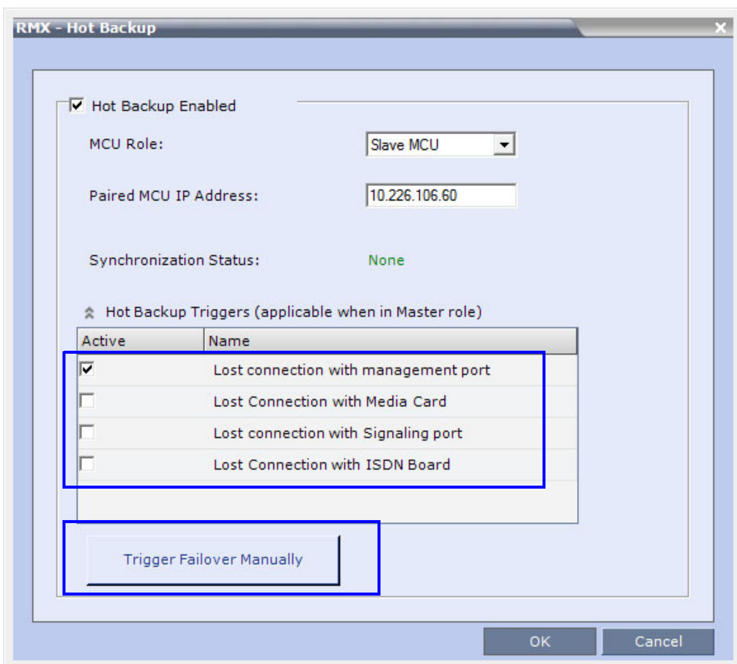
The *Hot Backup* triggers are configured in the *Hot Backup* dialog box for the Master MCU when the *Hot Backup* feature is enabled.



To add the Hot Backup triggers to the Hot Backup configuration:

1 In the *Hot Backup* dialog box, expand the **Trigger Hot Backup Triggers**.

A dialog box opens with a list of event triggers displayed.



2 Select the appropriate Hot Backup Triggers check boxes:

Table 21-5 Hot Backup Triggers

Hot Backup Trigger	Description
Lost connection with management port	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection to the management port is lost on the Master MCU. This trigger is always set.
Lost connection with media port	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection with an active media port is lost on the Master MCU.
Lost connection with signalling port	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection with an active signalling port is inactive for a duration of 30 seconds on the Master MCU. A system flag, ETH_INACTIVITY_DURATION, can be added and configured to modify the duration of inactivity of the signalling port. Default value is 30 seconds; Minimum value is 20 seconds.
Lost connection with ISDN card	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection with an ISDN card is disconnected on the Master MCU.

3 Alternatively, click the **Trigger Failover Manually** button when you want to trigger the Hot Backup manually and activate the Slave MCU.

A confirmation message is displayed.

4 Click **Yes** to continue the Hot Backup process or click **No** to cancel the Hot Backup process.

5 Click **OK**.

Modifications to the Master MCU Requiring System Reset

Modifications to the configuration of the *Master MCU* that require a *System Reset* cannot be performed while *Hot Backup* is enabled.

To modify the Master MCU configuration:

1 Disable the *Hot Backup* on the *Master* and *Slave* MCUs.

2 Modify the *Master MCUs* configuration.

3 Reset the *Master MCU.*

4 When the reset is complete, enable *Hot Backup* on the *Master* and *Slave MCU*s.

5 If required, reset the *Slave MCU.*

Audible Alarms

In addition to the visual cues used to detect events occurring on the RMX, an audible alarm can be activated and played when participants request Operator Assistance.

Using Audible Alarms

The Audible Alarm functionality for Operator Assistance requests is enabled for each MCU in either the *RMX Web Client* or *RMX Manager*.

The Audible Alarm played when Operator Assistance is requested is enabled and selected in the **Setup > Audible Alarm > User Customization**. When the Audible Alarm is activated, the *.wav file selected in the *User Customization* is played, and it is repeated according to the number of repetitions defined in the *User Customization*.

If more than one RMX is monitored in the *RMX Manager*, the Audible Alarm must be enabled separately for each RMX installed in the site/configuration. A different *.wav file can be selected for each MCU.

When multiple Audible Alarms are activated in different conferences or by multiple MCUs, the Audible Alarms are synchronized and played one after the other. It is important to note that when *Stop Repeating Alarm* is selected from the toolbar from the *RMX Web Client* or *RMX Manager*, all activated Audible Alarms are immediately halted.

Audible Alarm Permissions

An operator/administrator can configure the Request Operator Assistance audible alarm, however Users with different authorization level have different configuration capabilities as shown in Table 21-6.

Table 21-6 *Audible Alarm Permissions*

Option	Operator	Administrator
User Customization	✔	✔
Download Audible Alarm File		✔
Stop Repeating Alarms	✔	✔

Stop Repeating Message

The RMX User can stop playing the audible alarm at any time. If more than one audible alarm has been activated, all activated alarms are immediately stopped.

If after stopping the Audible Alarms a new Operator Assistance request event occurs, the audible alarm is re-activated.

To stop the Audible Alarm on the RMX Client or RMX Manager:

>> On the RMX menu, click **Setup** > **Audible Alarms** >**Stop Repeating Alarm**.

When selected all audible alarms are immediately stopped.

Configuring the Audible Alarms

User Customization

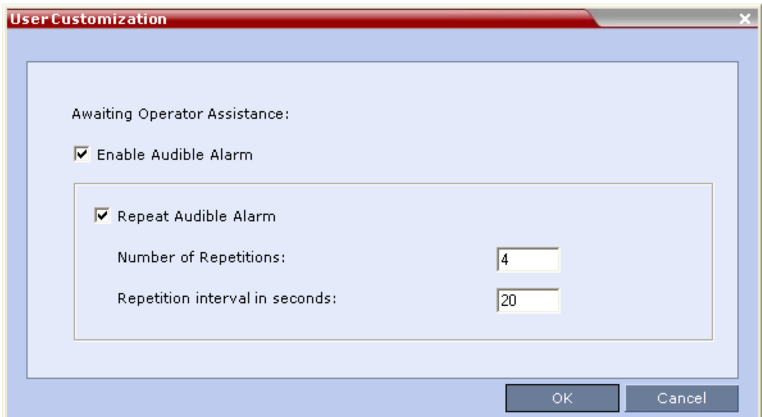
The operators and administrators can:

- Enable/Disable the Audible Alarm.
- Select whether to repeat the Audible Alarm.
- Define the number of repetitions and the interval between the repetitions.

To Customize the Audio Alert on the RMX Client or RMX Manager:

1 On the RMX menu, click **Setup** > **Audible Alarms** > **User Customization**.

The *User Customization* window opens.



2 Define the following parameters:

Table 21-7 Audible Alarm - User Customization Options

Option	Description
Enable Audible Alarm	Select this check box to enable the Audible Alarm feature and to define its properties. When this check box is cleared, the Audible Alarm functionality is disabled.
Repeat Audible Alarm	Select this check box to play the Audible Alarm repeatedly. When selected, it enables the definition of the number of repetitions and the interval between repetitions. When cleared, the Audible Alarm will not be repeated and will be played only once.
Number of Repetitions	Define the number of times the audible alarm will be played. Default number of repetitions is 4.
Repetition interval in seconds	Define the number of seconds that the system will wait before playing the Audible Alarm again. Default interval is 20 seconds.

3 Click **OK**.

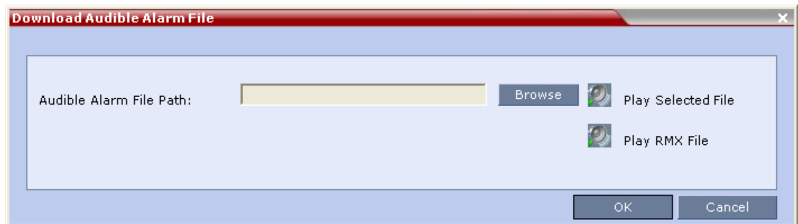
Replacing the Audible Alarm File

Each RMX is shipped with a default tone file in *.wav format that plays a specific tone when participants request Operator Assistance. This file can be replaced by a *.wav file with your own recording. The file must be in *.wav format and its length cannot exceed one hour.

Only the User with Administrator permission can download the Audible Alarm file.

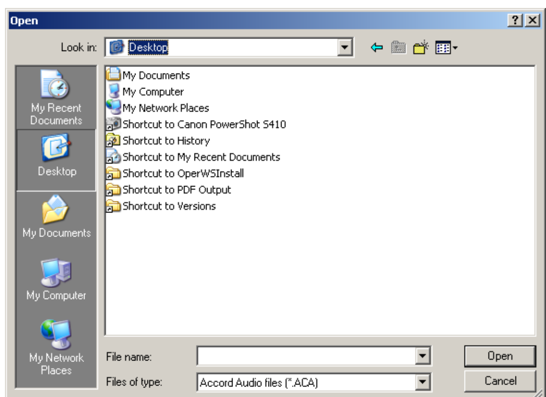
To replace the Audio file on the RMX Client or RMX Manager:

1 On the RMX menu, click **Setup** > **Audible Alarms** > **Download Audible Alarm File**. The *Download Audible Alarm File* window opens.



2 Click the **Browse** button to select the audio file (*.wav) to download.

The *Open* dialog box opens.



3 Select the appropriate *.wav file and then click the **Open** button. The selected file name is displayed in the *Install Audible Alarm File* dialog box.

4 **Optional**. You can play the selected file or the currently used file by clicking the *Play* ( ) button as follows:

a Click **Play Selected File** to play a file saved on your computer.

b Click **Play RMX File** to play the file currently saved on the RMX.

5 In the *Download Audible Alarm File* dialog box, click **OK** to download the file to the MCU.

The new file replaces the file stored on the MCU. If multiple RMXs are configured in the *RMX Manager*, the file must be downloaded to each of the required MCUs separately.

Multilingual Setting

Each supported language is represented by a country flag in the *Welcome Screen* and can be selected as the language for the *RMX Web Client.*

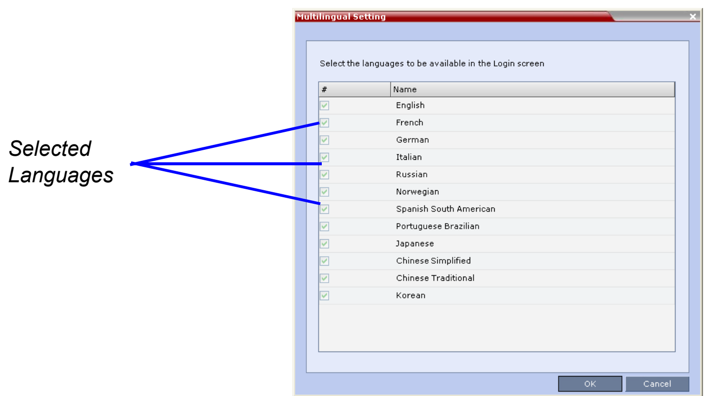
Customizing the Multilingual Setting

The languages available for selection in the *Login* screen of the *RMX Web Client* can be modified using the *Multilingual Setting* option.

To customize the Multilingual Setting:

1 On the RMX menu, click **Setup > Customize Display Settings > Multilingual Setting**.

The *Multilingual Setting* dialog box is displayed.



2 Click the check boxes of the languages to be available for selection.

3 Click **OK**.

4 **Log out** from the *RMX Web Client* and **Log in** for the customization to take effect**.**

Banner Display and Customization

The *Login Screen* and *Main Screen* of the *RMX Web Client* and the *RMX Manager can* display informative or warning text banners. These banners can include general information or they can be cautioning users to the terms and conditions under which they may log into and access the system, as required in many secured environments.

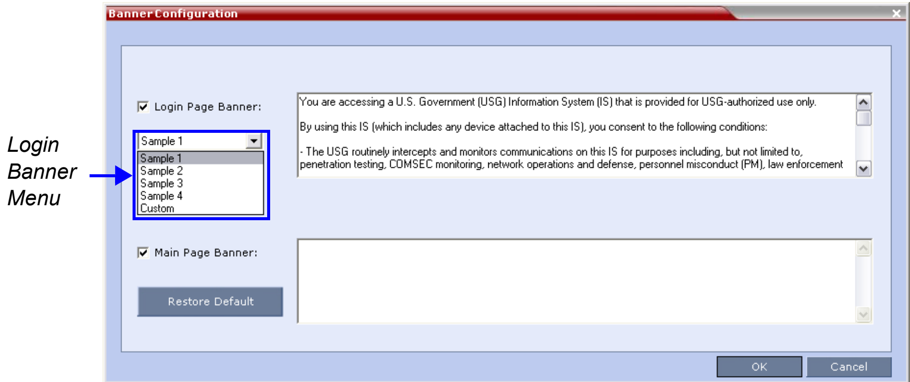
Banner display is enabled in the *Setup* > *Customize Display Settings* > *Banners Configuration*.

When the **ULTRA_SECURE_MODE** *System Flag* is set to **YES**, the banners are displayed by default and cannot be disabled. When set to **NO** (default), banner display is according to the check box selection in the *Banners Configuration* dialog box.

The administrator can choose one of four alternative login banners to be displayed. The four alternative banners cannot be modified. A *Custom* banner (default) can also be defined.

The *Main Page Banner* is blank and can be defined.

The *Banner Configuration* dialog box allows the administrator to select a *Login Banner* from a drop-down menu.



One of the the following *Login Banners* can be selected:

- **Non-Modifiable Banners**
  - *Sample 1*
  - *Sample 2*
  - *Sample 3*
  - *Sample 4*
- **Modifiable Banner**
  - *Custom* (Default)

Guidelines

- The *Login Banner* cannot be disabled when the RMX is in *Ultra Secure Mode*.
- The *Login Banner* must be acknowledged before the user is permitted to log in to the system.
- If a *Custom* banner has been created, and the user selects one of the alternative, non-modifiable banners the *Custom* banner not deleted.
- The *Custom Login Banner* banner may contain up to 1300 characters.
- An empty *Login Banner* is not allowed.
- Any attempt to modify a non-modifiable banner results in it automatically being copied to the *Custom* banner.

Non-Modifiable Banner Text

Sample 1 Banner

```
You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you
consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense,  personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
```

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Sample 2 Banner

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users also may be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Sample 3 Banner

You are about to access a system that is intended for authorized users only. You should have no expectation of privacy in your use of this system. Use of this system constitutes consent to monitoring, retrieval, and disclosure of any information stored within the system for any purpose including criminal prosecution.

Sample 4 Banner

This computer system including all related equipment, network devices (specifically including Internet access), is provided only for authorized use. All computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized personnel and their entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information including personal information, placed on or sent over this system may be monitored. Use of this system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of any such unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

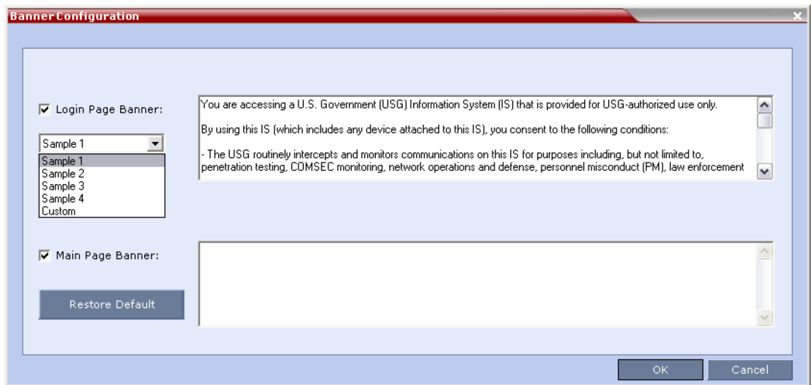
Customizing Banners

The *Login* and *Main Screen* banners can be customized to display conference information, assistance information or warning text as required in the *Ultra Secure Mode*.

To customize the banners:

1 In the RMX menu, click **Setup** > **Customize Display Settings** > **Banners Configuration**.

The *Banners Configuration* dialog box opens.



2 Customize the banners by modifying the following fields:

Table 21-8 *Banner Configuration*

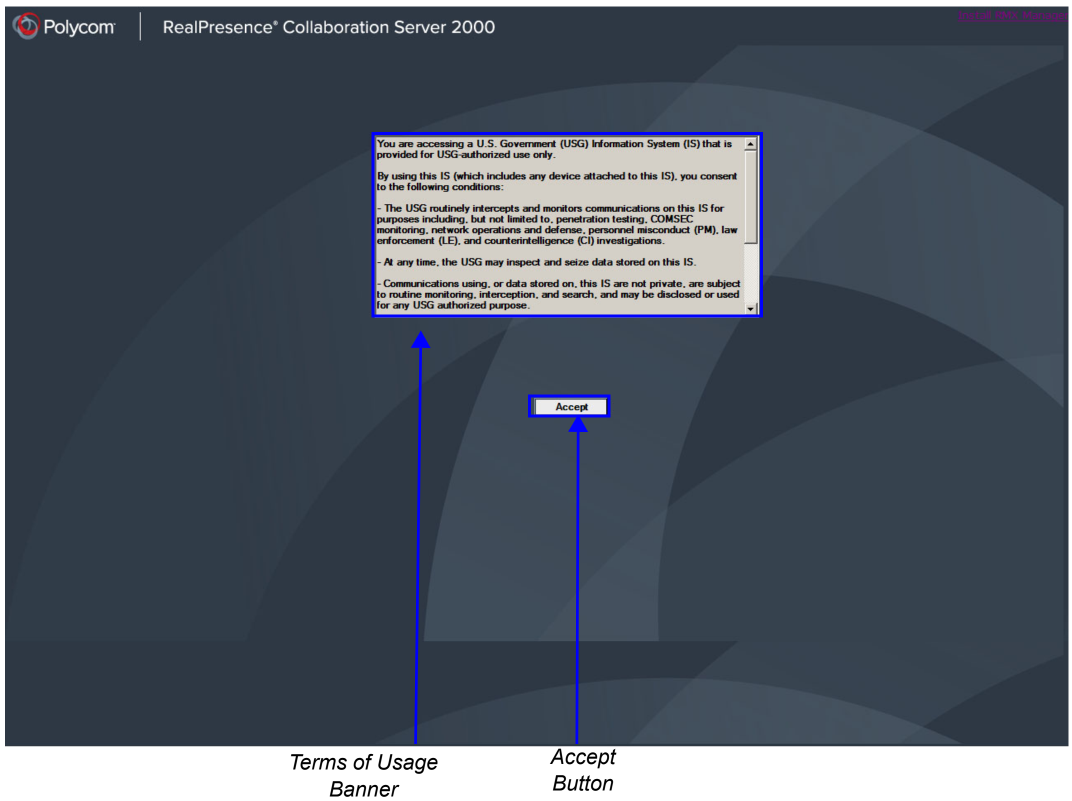
<table>
<tr><th rowspan="2">Field</th><th colspan="3">Description</th></tr>
<tr><th>Check Box</th><th>Text Field</th><th>Restore Default Button</th></tr>
<tr><td>Login Page Banner</td><td rowspan="2">Select or clear the check box to enable or disable the display of the banner.
Note: Banner display cannot be disabled in when the Ultra Secure_Mode flag is set to YES.</td><td rowspan="2">Edit the text in this field to meet local requirements:
• Banner content is multilingual and uses Unicode, UTF-8 encoding. All text and special characters can be used.
• Maximum banner size is 100KB.
• The banner may not be left blank when the Ultra Secure_Mode flag is set to YES.</td><td rowspan="2">Click the button to restore the default text to the banner</td></tr>
<tr><td>Main Page Banner</td></tr>
</table>

3 Click the **OK** button.

Banner Display

Login Screen Banner

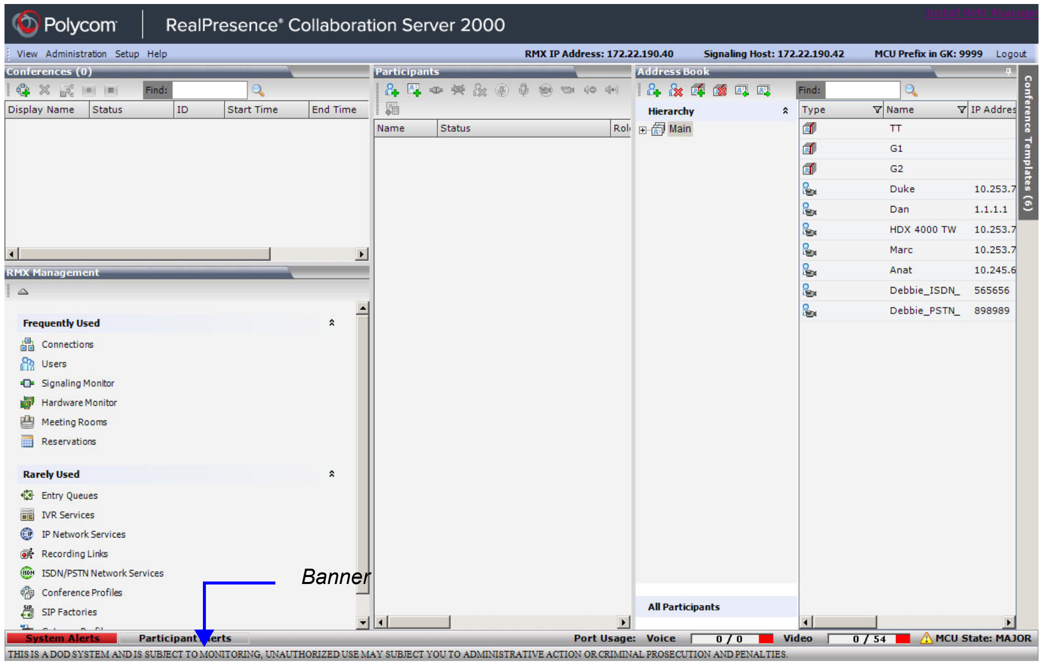
The *Login* screen banner can display any text, for example the terms and conditions for system usage (default text) that is required in the *Ultra Secure Mode*. The RMX User must acknowledge that the information was read and click the **Accept** button to proceed to the *Login* screen as shown in the following screen:



When the RMX is configured to work in *Ultra Secure Mode*, such as Maximum Security Environments, the display banner includes the terms and conditions for system usage as detailed in the default text: contained in *Sample Banner 1*.

Main Screen Banner

The *Main Screen* banner is displayed at the bottom of the screen, as follows:



When the RMX is configured to work in *Ultra Secure Mode*, such as the Maximum Security environment, the display banner includes the following default text:

```
THIS IS A DOD SYSTEM AND IS SUBJECT TO MONITORING, UNAUTHORIZED USE MAY
SUBJECT YOU TO ADMINISTRATIVE ACTION OR CRIMINAL PROSECUTION AND PENALTIES.
```

Software Management

The *Software Management* menu is used to backup and restore the RMX's configuration files and to download MCU software.

Backup and Restore Guidelines

- Direct access to the RMX file system is disabled in both *Ultra Secure Mode* and standard security mode.
- *System Backup* can only be performed by an administrator.
- The *System Backup* procedure creates a single backup file that can be viewed or modified only by developers.
- A *System Backup* file from one system can be restored on another system.
- To ensure file system consistency, do not perform any configuration changes as the system does not suspended them during the backup procedure.
- The following parameters, settings and files are backed up:
  — MCMS configuration files (/mcms/Cfg):
  — Network and service configurations,
  — Rooms,

— Profiles
— Reservations
— System Flags
— Resource Allocation
— IVR messages, music
— *RMX Web Client* user setting - fonts, windows
— *RMX Web Client* global settings – notes, address book, language
— Private keys and certificates (TLS)
— Conference participant settings
— Operation DB (administrator list)
— SNMP settings
— Time configuration

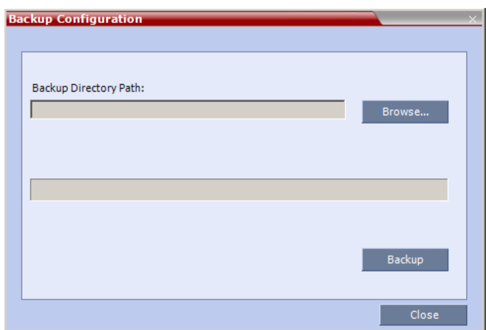
- CDR files are not included in the backup process and should be backed up manually by saving the CDR files to a destination device.

Using Software Management

To backup configuration files:

1 On the *RMX* menu, click **Administration > Software Management > Backup Configuration**.

The *Backup Configuration* dialog box opens.



2 **Click the Browse** button.
The Browse To File dialog box opens.

3 Select the *Backup Directory Path* and then click **Backup**.

> When the RMX system backs up the current configuration, if any changes occur immediately or during the request, then additional changes are not registered.

To restore configuration files:

1 On the *RMX* menu, click **Administration** > **Software Management** > **Restore Configuration**.

2 **Browse** to the *Restore Directory Path* where the backed up configuration files are stored and then click **Restore**.

To download MCU software files:

1 On the *RMX* menu, click **Administration** > **Software Management** > **Software Download**.

2 **Browse** to the *Install Path* and then click **Install**.

Ping RMX

The *Ping* administration tool enables the *RMX Signaling Host* to test network connectivity by *Pinging* IP addresses.

Guidelines

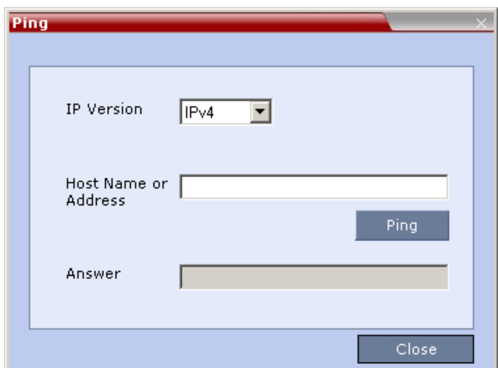
- The IP addressing mode can be either IPv4 or IPv6.
- Both explicit IP addresses and *Host Names* are supported.
- The *RMX Web Client* blocks any attempt to issue another *Ping* command before the current *Ping* command has completed. Multiple *Ping* commands issued simultaneously from multiple *RMX Web Client*s are also blocked.

Using Ping

To Ping a network entity from the RMX:

1 On the RMX menu, click **Administration > Tools > Ping**.

The *Ping* dialog box is displayed:



2 Modify or complete the following fields:

Table 21-9 *Ping*

Field	Description
IP Version	Select *IPv4* or *IPv6* from the drop-down menu.
Host Name or Address	Enter the *Host Name* or *IP Address* of the *network* entity to be *Pinged*.

3 Click the **Ping** button.

The *Ping* request is sent to the *Host Name* or *IP Address* of the RMX entity.

The *Answer* is either:

— *OK, or*

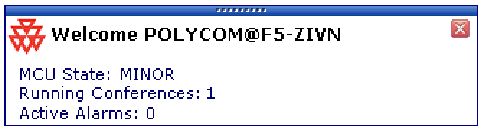
— *FAILED*

Notification Settings

The RMX can display notifications when:

- A new RMX user connects to the MCU.
- A new conference is started.
- Not all defined participants are connected to the conference or when a single participant is connected.
- A change in the MCU status occurs and an alarm is added to the alarm's list.

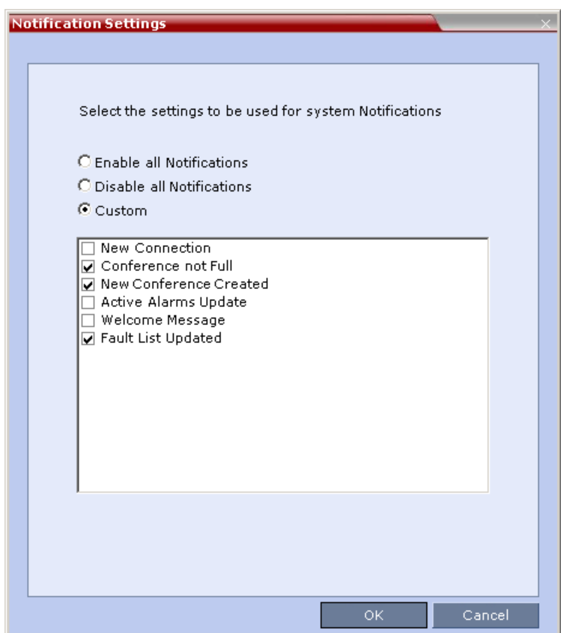
A welcome message is displayed to the RMX user upon connection.



To configure the notifications:

1 On the *RMX* menu, select **Setup** > **Notification Settings**.

The *Notification Settings* dialog box is displayed.



The following notification options are displayed.

***Table 21-10** Notification Settings Parameters*

Field	Description
New Connection	Notification of a new user/administrator connecting to the RMX.
New Conference Created	New conference has been created.
Conference Not Full	The conference is not full and additional participants are defined for the conference.

Table 21-10 *Notification Settings Parameters (Continued)*

Field	Description
Welcome Message	A welcome message after user/administrator logon.
Active Alarms Update	Updates you of any new alarm that occurred.
Fault List Updated	Updates you when the faults list is updated (new faults are added or existing faults are removed).

2 **Enable/Disable All Notifications** or **Custom** to select specific notifications to display.

3 Click **OK**.

Logger Diagnostic Files

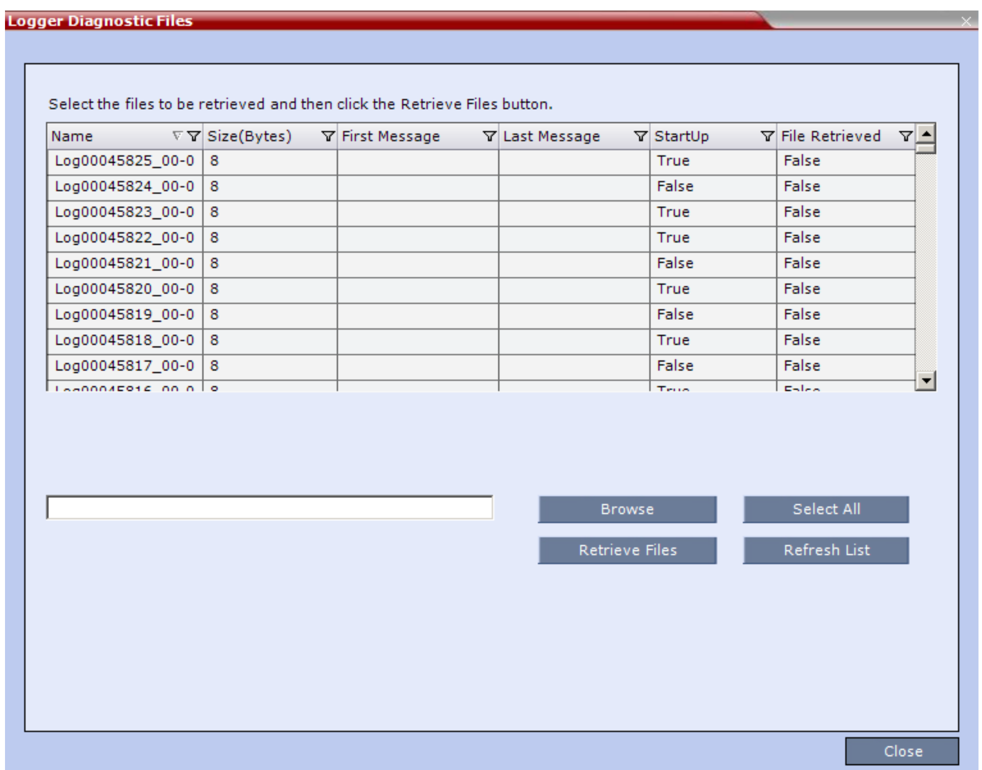
The Logger utility is a troubleshooting tool that continually records MCU system messages and saves them to files in the MCU hard drive. For each time interval defined in the system, a different data file is created. The files may be retrieved from the hard drive for off-line analysis and debugging purposes.

The Logger utility is activated at the MCU startup. The Logger is disabled when the MCU is reset manually or when there is a problem with the Logger utility, e.g. errors on the hard drive where files are saved. In such cases, data cannot be retrieved.

When the MCU is reset via the RMX, the files are saved on the MCU hard drive.

To access the Logger Diagnostic Files:

>> On the *RMX* menu, click **Administration > Tools > Logger Diagnostic Files**.



The following tasks can be performed:

Table 21-11 *Diagnostic File Button Options*

Button	Description
Refresh List	Refreshes the list and adds newly generated logger files.
Select All	Selects all the logger files listed.
Browse	Selects the destination folder for download.
Retrieve Files	Saves files to the destination folder.

When retrieved, the log file name structure is as follows:

- Sequence number (starting with 1)
- Date and Time of first message
- Date and Time of last message
- File size
- Special information about the data, such as Startup

File name structure:

Log_SNxxxxxxxxxx_FMDddmmyyy_FMThhmm_LMDddmmyyyy_LMThhmm_SZxxxxxxxxxx_SUY.log

File name format:

- SN = Sequence Number
- FM = First Message, date and time
- LM = Last Message, date and time
- SZ = Size
- SU = Startup (Y/N) during the log file duration

Example:

Log_SN0000000002_FMD06032007_FMT083933_LMD06032007_LMT084356_SZ184951_SUY.log.

Retrieving the Logger Files:

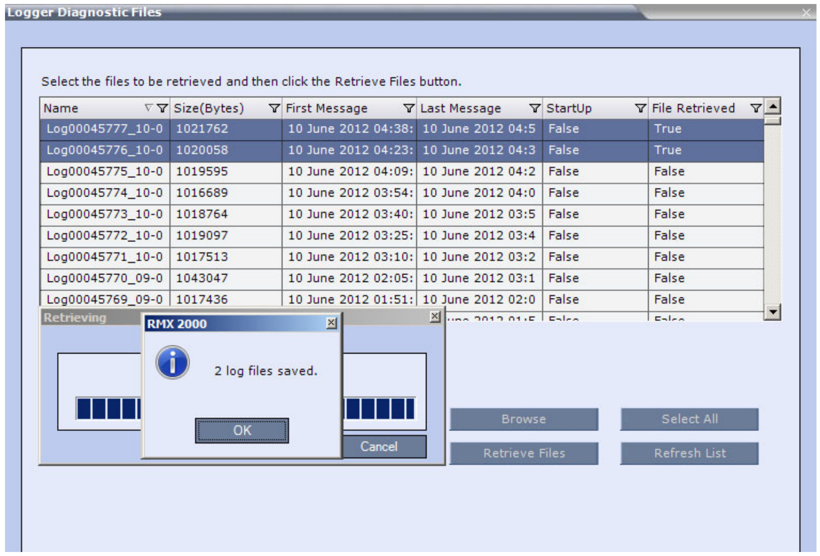
1 Select the log files to retrieve. Multiple selections of files are enabled using standard Windows conventions.

2 In the *Logger Diagnostic Files* dialog box, click the **Browse** button.

3 In the *Browse for Folder* window, select the directory location to save the Logger files and click **OK**.

You will return to the *Logger Diagnostic Files* dialog box.

4 Click the **Retrieve Files** button.



The log files (in *.txt format) are saved to the defined directory and a confirmation caption box is displayed indicating a successful retrieval of the log files.

Viewing the Logger Files:

To analyze the log files generated by the system, open the retrieved *.txt files in any text editor application, i.e. Notepad, Textpad or MS Word.

1 Using Windows Explorer, browse to the directory containing the retrieved log files.

2 Use any text editor application to open the log file(s).

Information Collector

Standard Security Mode

The Information Collector comprehensively attains all information from all the MCU internal entities for data analysis. That data, stored in a central repository, is logged from the following system components:

- System Log Files
- CDR
- OS (Core dumps, CFG - DNS, DHCP, NTP, kernal state, event logs
- Signaling Trace files (H.323 & SIP)
- Central Signaling logs
- Processes internal state and statistics
- Full faults
- Apache logs
- CFG directory (without IVR)
- Cards info: HW version, state and status
- SW version number

The data collected is saved into a single compressed file containing all the information from each system component in its relative format (.txt, .xml, etc...). In case the disk is malfunctioning, the file will be written to the RAM (involves only a small amount of information where the RAM size is 1/2 a gigabyte). The zipped file (info.tgz) can be opened with the following applications: WinRAR and WinZip. The entire zipped file is then sent to Polycom's Network Systems Division for analysis and troubleshooting.

Ultra Secure Mode

The *Information Collector* logs information from the RMX's *Network Intrusion Detection System* (*NIDS*), saving it into a compressed disk file. (If the disk malfunctions, the file is written to *RAM*.) The zipped file (*info.tgz*) can be opened with either *WinRAR* or *WinZip*. The entire zipped file can be sent to *Polycom* for analysis.

Network Intrusion Detection System (NIDS)

The RMX system uses iptables for access control. For each different kind of packet processing, there is a table containing chained rules for the treatment of packets. Every network packet arriving at or leaving from the RMX must pass the rules applicable to it.

Depending on the nature of the suspect packets, the rules may reject, drop, or limit their arrival rate (dropping the rest).

The RMX maintains a log that includes all unpermitted access attempts blocked by the fire wall.

Unpermitted access includes:

- Access to ports which are not opened on the RMX.
- Invalid access to open ports.

Using the Information Collector

When the *Information Collector* is used the following steps are performed:

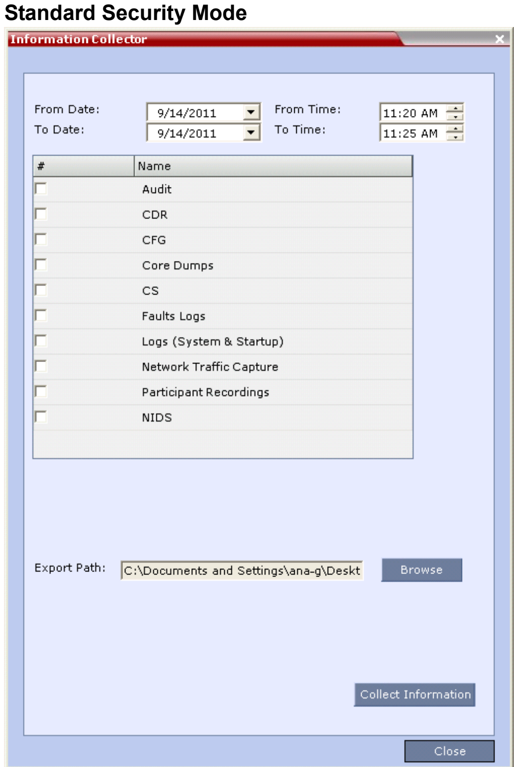
- **Step 1: Creating** the *Information Collector* file.
- **Step 2**: **Saving** the *Information Collector* file.
- **Step 3: Viewing** the information in the *Information Collector* file.

Step 1: Creating the Information Collector Compressed File

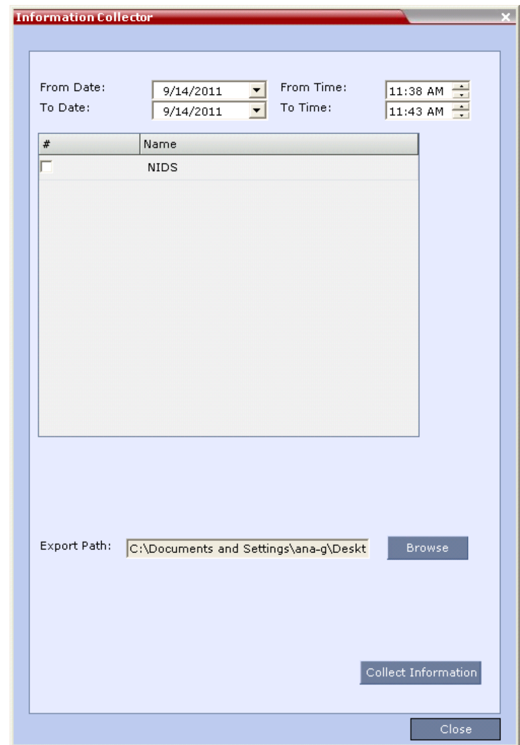
To create the compressed file:

1 In the RMX menu, click **Administration > Tools > Information Collector**.
The *Information Collector* dialog box is displayed.

Standard Security Mode



Ultra Secure Mode



2 In the *From Date* and *Until Date* fields, use the arrow keys to define the date range of the data files to be included in the compressed file.

3 In the *From Time* and *Until Time* fields, use the arrow keys to define the time range of the data files to be included in the compressed file.

4 Select check boxes of the information to be collected.

5 In the *Export Path* field, click the **Browse** button and navigate to the directory path where the compressed file is to be saved.

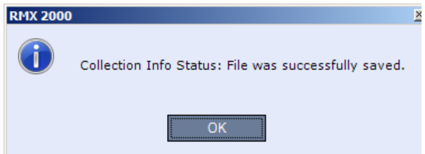
6 Click the **Collect Information** button.

A progress indicator is displayed in the *Information Collector* dialog box while the file is being created.

Step 2: Saving the Compressed File

1 The compressed file is automatically saved in the directory selected in the *Information Collector* dialog box. The file is named **info.tgz**.

A success information box is displayed.



2 Click the **OK** button.

Step 3: Viewing the Compressed File

The compressed file is saved in *.tgz* format and can be viewed with any utility that can open files of that format, for example *WinRAR® 3.80*.

To view the compressed file:

1 Navigate to the directory on the workstation in which the file was saved.

2 Double click the **info.tgz** file to view the downloaded information.

> Some browsers save the file as *info.gz* due to a browser bug. If this occurs, the file must be manually renamed to *info.tgz* before it can be viewed.

Auditor

An *Auditor* is a user who can view *Auditor* and *CDR* files for system auditing purposes.

> The *Auditor* user must connect to the RMX using the *RMX Web Client* only.

The *Event Auditor* enables administrators and auditors to analyze configuration changes and unusual or malicious activities in the RMX system.

Auditor operates in real time, recording all administration activities and login attempts from the following RMX modules:

- Control Unit
- Shelf Manager

For a full list of monitored activities, see Table 21-13 on page **21-65** and Table 21-14 on page **21-66**.

The *Auditor* must always be active in the system. A *System Alert* is displayed if it becomes inactive for any reason.

The *Auditor* tool is composed of the *Auditor Files* and the *Auditor File Viewer* that enables you to view the *Auditor Files*.

> Time stamps of *Audit Events* are GMT.

Auditor Files

Auditor Event History File Storage

All audit events are saved to a buffer file on hard disk in real time and then written to a file on hard disk in XML in an uncompressed format.

A new current auditor event file is created when:

- the system is started
- the size of the current auditor event file exceeds 2 MB
- the current auditor event file's age exceeds 24 hours

Up to 1000 auditor event files are stored per RMX. These files are retained for at least one year and require 1.05 GB of disk space. The files are automatically deleted by the system (oldest first) when the system reaches the auditor event file limit of 1000.

A *System Alert* is displayed with *Can't store data* displayed in its *Description* field if:

- the system cannot store 1000 files
- the RMX does not have available disk space to retain files for one year

Audit Event Files are retained by the RMX for at least 1 year. Any attempt to delete an audit event file that is less than one year old raises a *System Alert* with *File was removed* listed in the *Description* field.

Using the *Restore Factory Defaults* of the *System Restore* procedure erases *Audit Files*.

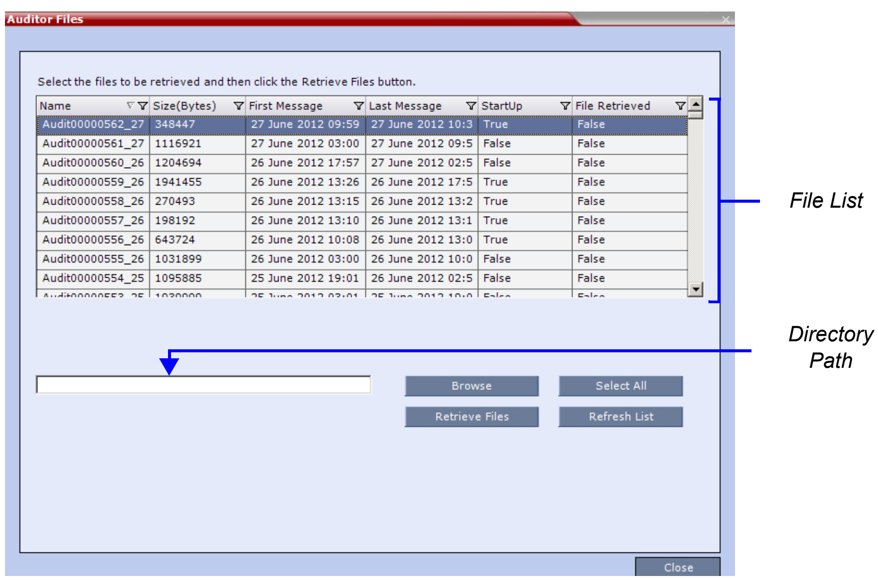
Retrieving Auditor Files

You can open the *Auditor* file directly from the *Auditor Files* list or you can retrieve the files and save them to a local workstation.

To access Auditor Files:

>> On the RMX menu, click **Administration > Tools > Auditor Files**.

The *Auditor Files* dialog box is displayed.



The *Auditor Files* dialogue box displays a file list containing the following file information:

— *Name*

— Size (Bytes)
— *First Message* – date and time of the first audit event in the file
— *Last Message* – date and time of the last audit event in the file
— StartUp:
  - *True* – file was created when the system was started
  - *False* – file was created when previous audit event file reached a size of 2 MB or was more than 24 hours old
— File Retrieved:
  - *True* - file was previously retrieved.
  - *False* - file was never previously retrieved.

The order of the *Auditor Files* dialog box field header columns can be changed and the fields can be filtered to enable searching.

For more information, see "*Auditor File Viewer”* on page **21-62**.

To retrieve files for storage on a workstation:

1 Click **Browse** and select the folder on the workstation to receive the files and then click **OK**.

The folder name is displayed in the directory path field.

2 Select the file(s) to be retrieved by clicking their names in the file list or click **Select All** to retrieve all the files. (Windows multiple selection techniques can be used.)

3 Click Retrieve Files.

The selected files are copied to the selected directory on the workstation.

To open the file in the Auditor File Viewer:

>> Double-click the file.

Auditor File Viewer

The *Auditor File Viewer* enables *Auditors* and *Administrators* to view the content of and perform detailed analysis on auditor event data in a selected *Auditor Event File*.

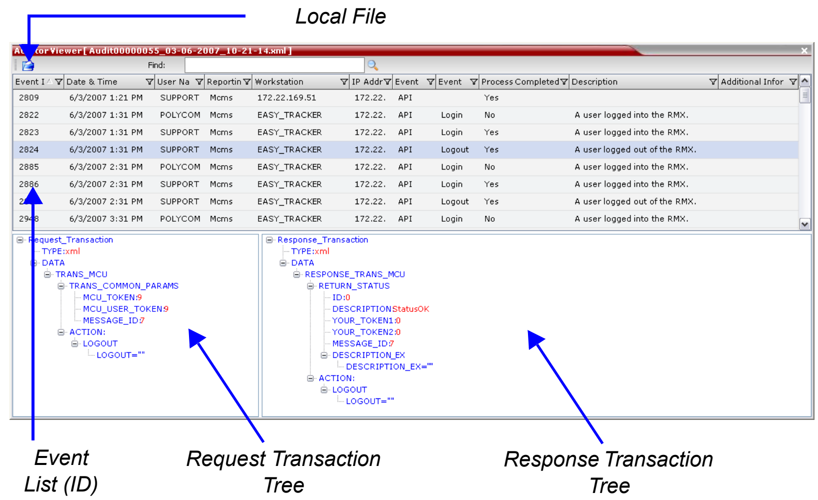
You can view an *Auditor Event File* directly from the *Auditor Files* list or by opening the file from the *Auditor File Viewer*.

To open the Auditor File Viewer from the Administration Menu:

1 On the RMX menu, click **Administration > Tools > Auditor File Viewer**.

The *Auditor File Viewer* is displayed.

If you previously double clicked an *Auditor Event File* in the *Auditor Files* list, that file is automatically opened.



The following fields are displayed for each event:

Table 21-12 *Auditor Event Columns*

Field	Description
Event ID	The sequence number of the event generated by the RMX.
Date & Time	The date and time of the event taken from the RMX's *Local Time* setting.
User Name	The *Username* (Login Name) of the user who triggered the event.
Reporting Module	The RMX system internal module that reported the event: • MCMS • MPL • Central Signaling • MPL Simulation • RMX Web Client • CM Switch • Shelf Management • ART • Video • Card Manager • RTM • MUX
Workstation	The name (alias) of the workstation used to send the request that triggered the event.
IP Address (Workstation)	The IP address of the workstation used to send the request that triggered the event.

Table 21-12 *Auditor Event Columns (Continued)*

Field	Description
Event Type	Auditor events can be triggered by: • API • HTTP • RMX Internal Event
Event	The process, action, request or transaction that was performed or rejected. • POST:SET transactions (API) • Configuration changes via XML (API) • Login/Logout (API) • GET (HTTP) • PUT (HTTP) • MKDIR (HTTP) • RMDIR (HTTP) • Startup (RMX Internal Event) • Shutdown (RMX Internal Event) • Reset (RMX Internal Event) • Enter Diagnostic Mode (RMX Internal Event) • IP address changes via USB (RMX Internal Event)
Process Completed	Status of the process, action, request or transaction returned by the system: • Yes – performed by the system. • No – rejected by the system.
Description	A text string describing the process, action, request or transaction.
Additional Information	An optional text string describing the process, action, request or transaction in additional detail.

The order of the *Auditor File Viewer* field header columns can be changed and the fields can be sorted and filtered to facilitate different analysis methods.

2 In the event list, click the events or use the keyboard's Up-arrow and Down-arrow keys to display the *Request Transaction* and *Response Transaction* XML trees for each audit event.

The transaction XML trees can be expanded and collapsed by clicking the expand (+) and collapse (−) buttons.

To open an auditor event file stored on the workstation:

1 Click the **Local File** button ( ) to open the *Open* dialogue box.

2 Navigate to the folder on the workstation that contains the audit event file.

3 Select the audit event file to be opened.

4 Click **Open**.

The selected file is opened in the *Auditor Viewer*.

Audit Events

Alerts and Faults

Table 1 lists *Alerts* and *Faults* that are recorded by the *Auditor*.

Table 21-13 *Alerts and Faults*

Event
Attempt to exceed the maximum number of management session per user
Attempt to exceed the maximum number of management sessions per system
Central Signaling indicating Recovery status.
Failed login attempt
Failed to open Apache server configuration file.
Failed to save Apache server configuration file.
Fallback version is being used.
File system scan failure.
File system space shortage.
Internal MCU reset.
Internal System configuration during startup.
Invalid date and time.
Invalid MCU Version.
IP addresses of Signaling Host and Control Unit are the same.
IP Network Service configuration modified.
IP Network Service deleted.
Login
Logout
Management Session Time Out
MCU Reset to enable Diagnostics mode.
MCU reset.
Music file error.
New activation key was loaded.
New version was installed.
NTP synchronization failure.
Polycom default User exists.
Private version is loaded.

Table 21-13 Alerts and Faults (Continued)

Event
Restoring Factory Defaults.
Secured SIP communication failed.
Session disconnected without logout
SSH is enabled.
System Configuration modified.
System is starting.
System Resets.
TCP disconnection
Terminal initiated MCU reset.
The Log file system is disabled.
The software contains patch(es).
USB key used to change system configuration.
User closed the browser
User initiated MCU reset.

Transactions

Table 2 lists *Transactions* that are recorded by the *Auditor*.

Table 21-14 Transactions

Transaction
TRANS_CFG:SET_CFG
TRANS_IP_SERVICE:DEL_IP_SERVICE
TRANS_IP_SERVICE:NEW_IP_SERVICE
TRANS_IP_SERVICE:SET_DEFAULT_H323_SERVICE
TRANS_IP_SERVICE:SET_DEFAULT_SIP_SERVICE
TRANS_IP_SERVICE:UPDATE_IP_SERVICE
TRANS_IP_SERVICE:UPDATE_MANAGEMENT_NETWORK
TRANS_ISDN_PHONE:ADD_ISDN_PHONE
TRANS_ISDN_PHONE:DEL_ISDN_PHONE
TRANS_ISDN_PHONE:UPDATE_ISDN_PHONE
TRANS_ISDN_SERVICE:DEL_ISDN_SERVICE
TRANS_ISDN_SERVICE:NEW_ISDN_SERVICE

Table 21-14 *Transactions (Continued)*

Transaction
TRANS_ISDN_SERVICE:SET_DEFAULT_ISDN_SERVICE
TRANS_ISDN_SERVICE:UPDATE_ISDN_SERVICE
TRANS_MCU:BEGIN_RECEIVING_VERSION
TRANS_MCU:COLLECT_INFO
TRANS_MCU:CREATE_DIRECTORY
TRANS_MCU:FINISHED_TRANSFER_VERSION
TRANS_MCU:LOGIN
TRANS_MCU:LOGOUT
TRANS_MCU:REMOVE_DIRECTORY
TRANS_MCU:REMOVE_DIRECTORY_CONTENT
TRANS_MCU:RENAME
TRANS_MCU:RESET
TRANS_MCU:SET_PORT_CONFIGURATION
TRANS_MCU:SET_RESTORE_TYPE
TRANS_MCU:SET_TIME
TRANS_MCU:TURN_SSH
TRANS_MCU:UPDATE_KEY_CODE
TRANS_OPERATOR:CHANGE_PASSWORD
TRANS_OPERATOR:DELETE_OPERATOR
TRANS_OPERATOR:NEW_OPERATOR
TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN
TRANS_SNMP:UPDATE

ActiveX Bypass

At sites that, for security reasons, do not permit Microsoft® ActiveX® to be installed, the MSI (Windows Installer File) utility can be used to install .NET Framework and .NET Security Settings components on workstations throughout the network.

All workstation that connect to RMX systems must have both.NET Framework and .NET Security Settings running locally. These components are used for communication with the RMX and can only be installed on workstations by users with administrator privileges.

The MSI utility requires the IP addresses of all the RMX systems (both control unit and Shelf Management IP addresses) that each workstation is to connect to.
If the IP address of the any of the target RMXs is changed, the ActiveX components must be reinstalled.

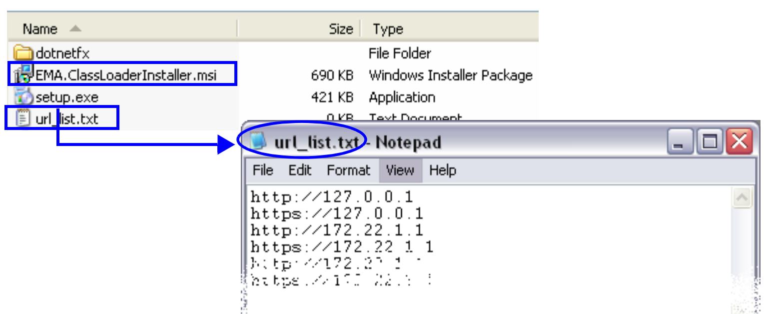
Installing ActiveX

To install ActiveX components on all workstations in the network:

1 Download the MSI file **EMA.ClassLoaderInstaller.msi** from the Polycom Resource Center.
The MSI file contains installation scripts for both .NET Framework and .NET Security Settings.

2 Create a text file to be used during the installation containing the IP addresses of all the RMX systems (both control unit and Shelf Management IP addresses) that each workstation in the network is to connect to.

The file must be named **url_list.txt** and must be saved in the same folder as the downloaded MSI file.



3 Install the ActiveX components on all workstations on the network that connect to RMX systems.

The installation is done by the network administrator using a 3rd party network software installation utility and is transparent to all other users.

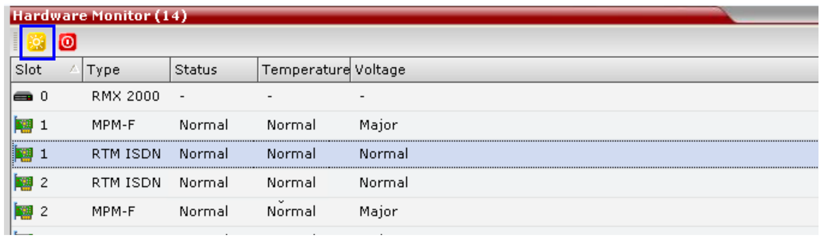
Resetting the RMX

System Reset saves system configuration changes and restarts the system with the latest settings.

To reset the RMX:

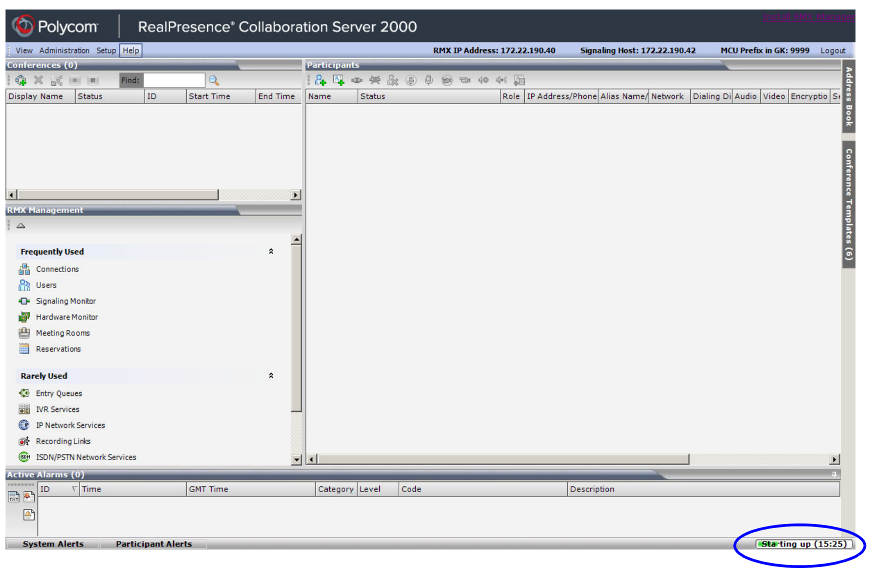
1 In the *RMX Management* pane, click the **Hardware Monitor button**.

The *Hardware Monitor* pane is displayed.

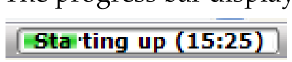


2 Click the **Reset** ( ) button.

When the RMX system is reset, during RMX startup the *Progress Bar* appears at the bottom of the RMX *Status* pane.



The progress bar displays the amount of time remaining for the reset process to complete:



. The *Startup* progress is also indicated by a green bar moving from left to right.

The duration of the *Startup* depends on the type of activity that preceded the MCU reset. For example: Fast Configuration Wizard, New Version installation, Version Upgrade, Restore Last Configuration etc.

> When resetting the RMX from the Hardware Monitor, sometimes SIP endpoints may remain connected, although the conference ended.

Restore Factory Defaults

You can erase the current RMX configuration and restore default factory settings. There are two Restore levels:

- Standard Restore
- Comprehensive Restore

This tool is intended for Administrator users, to be performed prior to RMA.

Standard Restore

The Standard Restore level (default setting) deletes the following files:

- CDR
- Address Book
- Log Files
- Faults
- Dump Files
- Notes

In addition all the conferencing entities are deleted:

- Entry Queues
- Profiles
- Meeting Rooms
- IVR Services
- Default Network IP Service

When the system is restarted, these conferencing entities are created based on the factory defaults. In addition, the *Fast Configuration Wizard* automatically opens, letting the user to define the Default IP Network Service.

Comprehensive Restore

In addition to the *Standard Restore*, the system deletes the:

- CFS license information
- Management Network Service

The MCU is restored to the settings it had when shipped from the factory. The *Product Activation Key* is required to re-configure the *Management Network Service* during the *First Entry Configuration.*

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, Chapter 2 "Procedure 2: Product Registration"* on page **2-20**.

Restoring Factory Defaults

Restoring the RMX to *Factory Defaults* can be performed using the:

- **Administration Tools in the RMX menu**

  This method is used when the user can login with *Administrator* or *Support* system permissions.

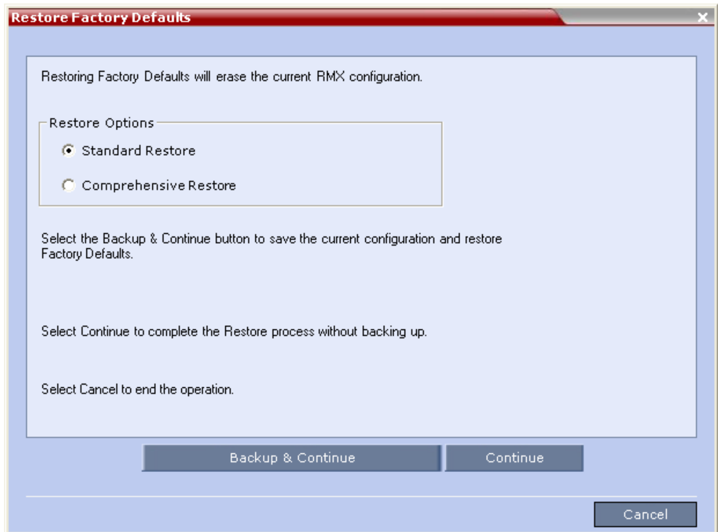
- **USB key**

  This method is used when the user cannot login with *Administrator* or *Support* system permissions.

To Restore Factory Default Settings using Administration Tools in the RMX menu:

1 In the RMX menu, click **Administration** > **Tools** > **Restore Factory Defaults.**

The *Restore Factory Defaults* dialog box appears.



2 Select **Standard Restore** or **Comprehensive Restore.**

If the current conferencing entities and system configuration are to be restored after restoring the initial system settings it is recommended to use the *Backup & Continue* option.

3 Click one of the following buttons:

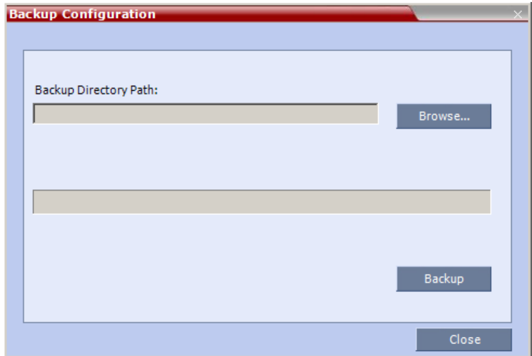
— **Backup & Continue** - Backup of the current RMX configuration. Proceed with step 4.

— **Continue** - Initializes all the current system configuration files and conferencing entities and then restores them to their factory values according to the selected restore level.
Proceed with step 5.

— **Cancel** - Cancels and exits this dialog box.

4 Click the **Backup & Configuration** option.

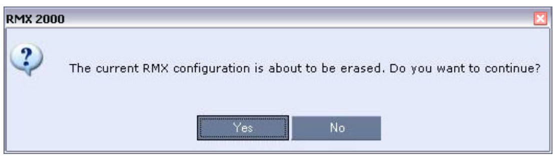
The *Backup Configuration Dialog* box opens.



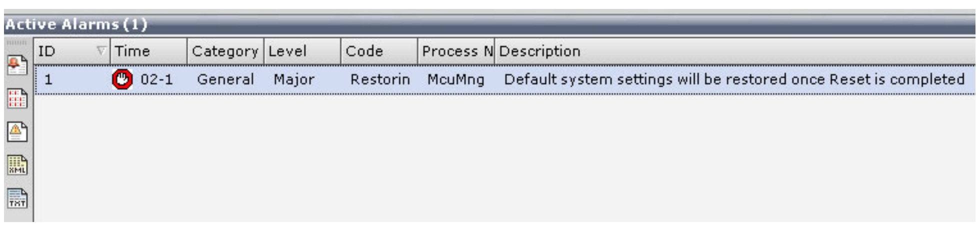
a Click **Browse** to select the *Backup Directory Path* and select **Backup**. The system initiates the backup of RMX configuration files.

b Optional. To exit click **Close**.

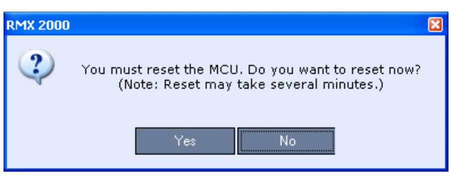
5 When the **backup** completes, a confirmation dialog box is displayed.



6 Click **Yes** to restore the RMX.
An *Active Alarm* is activated.



7 Click **Yes**, to reset the RMX.



8 Login to the RMX using the *Web Client*, if you selected:

— **Standard Restore**, the *Fast Configuration Wizard* appears. For more information, see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "Procedure 4: Modifying the Default IP Service and ISDN/PSTN Network Service Settings"* on page 2-28.

— **Comprehensive Restore**, requires initializing the *First Entry Configuration* procedures, as defined in the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide, "Procedure 1: First-time Power-up"* on page 2-25.

To Restore Factory Default Settings using the USB key:

> Restoring to factory defaults using the USB key method always results in a Comprehensive Restore. Obtain the *RestoreToFactoryDefault.txt* file from you next level of support and add it to the USB key.

1. Insert the *USB key in* the workstation.
2. Check that the *lan.cfg* file on the *USB key* contains the correct settings for the *Management Network Service.*
3. Verify that the *USB key* called includes the *RestoreToFactoryDefault.txt* file.
4. Power the RMX **Off.**
5. Remove the *USB key* from the workstation and insert it in the USB port on the RMX's back panel.
6. Power the RMX **On.**
7. In the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide,* follow "*Procedure 1: First-time Power-up"* on page **2-25**.

22

System Configuration Flags

The system's overall behavior can be configured by modifying the default values of the System Flags.

For flag changes (including deletion) to take effect, the MCU must be reset. For more information, see "*Resetting the RMX"* on page **21-69**.

The following *System Flags* do not require an MCU reset:

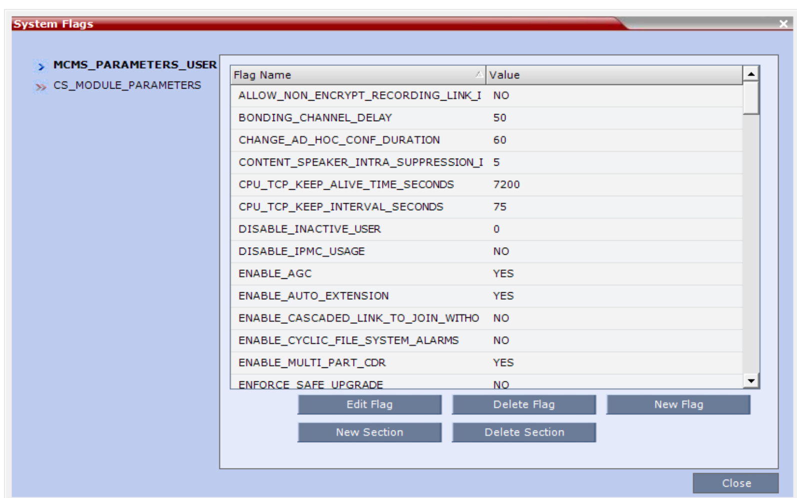
- IVR_MESSAGE_VOLUME
- IVR_MUSIC_VOLUME
- IVR_ROLL_CALL_VOLUME

Modifying System Flags

To modify system flags:

1 On the *RMX* menu, click **Setup > System Configuration**.

The *System Flags* dialog box opens.



2 In the *MCMS_PARAMETERS* tab, the following flags can be modified:

Table 22-1 *System Flags – MCMS_PARAMETERS*

Flag	Description
ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF	If YES, allows non-encrypted participants to connect to encrypted conferences. Default: No **Note:** From Version 7.6.1, this flag is replaced by the *Encryption* option *"Encrypt when Possible"* in the conference *Profile - Advanced* dialog box. Flag setting is ignored.
ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF	When set to **NO** (default), the Recording Link inherits the encryption settings of the conference. If the conference is encrypted, the recording link will be encrypted. When set to **YES**, it disables the encryption of the recording link, regardless of the Encryption settings of the conference and RSS recorder.
AUTHENTICATE_USER	This flag is not supported from Version 7.7. If the external database application is to be used to verify that operators are authorized to log in to the MCU, set the value of this flag to **YES**. If the value of this flag is set to **NO**, the MCU database is used to verify that operators are authorized to log in to the MCU. **Note:** If the flag is set to **YES,** the flow is first to look in the internal DB and then go out to the external one. Flags for SE200 need to be added manually.
BONDING_CHANNEL_DELAY (ISDN)	When connecting a bonding group, this is the delay (number of 1/100 seconds) between dialing attempts to connect sequential channels. The channel per second connection performance of ISDN switches can vary and can cause timing issues that result in bonding channel disconnection. Default: 6
CHANGE_AD_HOC_CONF_DURATION	The duration of an ad-hoc conference* can be configured on a system level by setting the flag to one of the following values (in minutes): **60** (default), **90**, **180** and **270**. * An ad-hoc conference is automatically created when the participant dials into an Ad-hoc Entry Queue and enters a conference ID that is not being used by any other conferencing entity. It is based on the Conference Profile assigned to the EQ.
CHECK_ARPING	This flag is not supported from Version 7.7. Disables *Duplicate Address Detection* and should be configured according to local site policy. When set to **YES**, *Duplicate Address Detection* is enabled in for both *IPv4* and *IPv6*. When set to **NO**, *Duplicate Address Detection* is disabled for both *IPv4* and *IPv6*. When using *IPv6*, *ICMPv6 type 135* packets are also disabled.

Table 22-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
CONTENT_SLAVE_LINKS_INTRA_SUPPRESSION_IN_SECONDS	Defines the interval, in seconds, during which the RMX is allowed to forward an *Intra Request* received from any of the *Slave Cascading Links.* The *Slave Cascading Link* can be connected to the local RMX, to an MCU on a higher cascade level or to the *Content* sharer. The first *Intra* request that is received from any of the *Slave MCUs* connected to the RMX starts the interval counter and is forwarded to the next level *MCU* or to the *Content* sharer. All other *Intra* requests that are received within this interval are registered but ignored. After an interval of <flag value> seconds, the system checks if during the last interval any additional *Intra* requests were registered. If there is at least one *Intra* request it will be forwarded. If there is no additional *Intra* request not no action is taken other than to wait for the next cycle. This filtering process is repeated every <flag value> seconds. **Default:** 30
CONTENT_SPEAKER_INTRA_SUPPRESSION_IN_SECONDS	This flag controls the requests to refresh (intra) the content sent from the RMX system to the content sender as a result of refresh requests initiated by other conference participants. Enter the interval in seconds between the Intra requests sent from the RMX to the endpoint sending the content to refresh the content display. Refresh requests that will be received from endpoints within the defined interval will be postponed to the next interval. Default setting: 5
CPU_TCP_KEEP_ALIVE_TIME_SECONDS	This flag indicates when to send the first KeepAlive indication to check the TCP connection. Default value: **7200** second (120 minutes) Range: 600-18000 seconds When there are NAT problems, this default may be too long and the TCP connection is lost. In such a case, the default value should be changed to 3600 seconds (60 minutes) or less.
CPU_TCP_KEEP_INTERVAL_SECONDS	This flag indicates the interval in seconds between the KeepAlive requests. Default value: **75** second Range: 10-720 seconds.
DISABLE_INACTIVE_USER	Users can be automatically disabled by the system when they do not log into the RMX application for a predefined period. Possible Values: **0** - **90** days. Default: **0** (disables this option). Default (ULTRA_SECURE_MODE=YES): 30

Table 22-1 System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
ENABLE_AGC	Set this flag to YES to enable the AGC option. (Default setting is NO.) When disabled, selecting the AGC option in the *Participant Properties* has not effect on the participant audio. For more information see "*Managing the Address Book"* on page 8-7. The Auto Gain Control mechanism regulates noise and audio volume by keeping the received audio signals of all participants balanced. **Note:** Enabling AGC may result in amplification of background noise.
ENABLE_AUTO_EXTENSIO N	When set to YES, allows conferences running on the RMX to be automatically extended as long as there are participants connected and the system has free resources. Set this flag to NO prevent conference duration from being automatically extended. It can also be used to enable the definition of conference duration that is shorter than is 11 minutes for the RealPresence Collaboration Server (RMX) 1500 and 20 minutes for the RMX 2000/4000. Default: YES
ENABLE_CASCADED_LINK _TO_JOIN_WITHOUT_PASS WORD	Enables a cascaded link to enter a conference without a password. Default: NO, for security reasons.
ENABLE_CYCLIC_FILE_SY STEM_ALARMS	Enables or disables the display of Active Alarms before overwriting the older CDR/Auditor/Log files, enabling the users to backup the older files before they are deleted. Default: NO Default (ULTRA_SECURE_MODE=YES): YES
ENFORCE_SAFE_UPGRAD E	When set to YES this flag enables the RMX system to notify users when an incorrect version upgrade/downgrade or upgrade/downgrade path is selected. When set to NO, after initiating an upgrade or downgrade software installation, the RMX activates a fault alert in the Faults List: “Warning: Upgrade started and SAFE Upgrade protection is turned OFF” and the upgrade/downgrade process continues. Range: YES / NO Default: YES
EXT_DB_IVR_PROV_TIME_ SECONDS	When an Entry Queue is set as IVR Service Provider for the DMA, the value here indicates the time interval in seconds in which the database is accesses for the ID. Default: 300

Table 22-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	**Description**
FORCE_CIF_PORT_ALLOCATION	Sets the MCU to allocate one CIF video resource to an endpoint, regardless of the resolution determined by the Conference Profile parameters. You can specify the endpoint types for which resource allocation can be forced to CIF resource, enabling other types of endpoints to use higher resolutions in the same conference. Enter the product type to which the CIF resource should be allocated. Possible values are: • **CMA Desktop -** for CMA desktop client • **VSX nnnn** - where nnnn represents the model number for example, VSX 8000.
FORCE_STRONG_PASSWORD_POLICY	When set to YES (default when ULTRA_SECURE_MODE=YES), implements the Strong Password rules. For more details, see "*Implementing Strong Passwords"* on page **15-10**. Default: NO
FORCE_SYSTEM_BROADCAST_VOLUME	If set to YES, the level of broadcasting volume of the connected participant is value taken from the system flag SYSTEM_BROADCAST_VOLUME. If set to NO (default), the broadcasting volume level is 5.
FORCE_SYSTEM_LISTENING_VOLUME	If set to YES, the level of listening volume of the connected participant is value taken from the system flag SYSTEM_LISTENING_VOLUME. If set to NO (default), the listening volume level is 5.
GK_MANDATORY_FOR_CALLS_IN	If set to **YES**, a gatekeeper is required to receive incoming H.323 calls. If a gatekeeper is not configure in the RMX, the calls will fail. If set to **NO** (default), gatekeeper is not required to process H.323 incoming calls and H.323 participants can dial in with or without a gatekeeper.
GK_MANDATORY_FOR_CALLS_OUT	If set to **YES**, a gatekeeper is required to perform H.323 outgoing calls. If a gatekeeper is not configure on the RMX, the calls will fail. If set to **NO** (default), gatekeeper is not required to dial out to H.323 participants and calls can be dialed out with or without a gatekeeper.
H263_ANNEX_T	Set to NO to send the content stream without Annex T and enable Aethra and Tandberg endpoints, that do not support Annex T, to process the content. Default: YES
HD_THRESHOLD_BITRATE	Sets the minimum bit rate required by endpoints to connect to an HD Conference. Endpoints that cannot support this bit rate are connected as audio only. Range: 384kbps - 4Mbs (Default: 768)

Table 22-1 System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
HIDE_SITE_NAMES	From version 7.6.1, in ***MPMx** Card Configuration Mode*, this *flag* has been replaced by the *Enable Site Names* option in the *Conference Profile - Site Names* dialog box. It allows you to enable or disable the display of site names in conferences per conference. From Version 7.6, in ***MPM+** Card Configuration Mode*, this *flag* has been replaced by the *Site Names* option in the *Conference Properties - Video Settings* dialog box. It allows you to enable or disable the display of site names in conferences per conference. In versions prior to 7.6, set this flag to ON to cancel the display of site names. When set to ON and the display is disabled, the flag SITE_NAMES_ALWAYS_ON =YES is ignored. Default: OFF **Note:** This option is unavailable in VSW conferences.
INTERNAL_SCHEDULER	When set to NO (default) this flag prevents potential scheduling conflicts from occurring as a result of system calls from external scheduling applications such as Polycom ReadiManager®, CMA™ 4000/5000 and others via the API. Set to YES to schedule conference reservations using an external scheduling application.
ISDN_COUNTRY_ CODE	The name of the country in which the MCU is located. Default: COUNTRY_NIL
ISDN_IDLE_CODE_E1	The Idle code (silent), transmitted on the ISDN E1 B channels, when there is no transmission on the channels. Default: 0x54
ISDN_IDLE_CODE_T1	The Idle code (silent), transmitted on the ISDN T1 B channels, when there is no transmission on the channels. Default: 0x13
ISDN_LEGACY_EP_CLOSE _CONTENT_FORCE_H263	If set to YES, legacy ISDN endpoints that do not support sharing content over the Content channel receive video over video channel that is forced to H.263 video. Default: NO.
ISDN_NUM_OF DIGITS	When using ISDN Overlap sending dialing mode, this field holds the number of digits to be received by the MCU. Default: 9

Table 22-1 *System Flags – MCMS_PARAMETERS (Continued)*

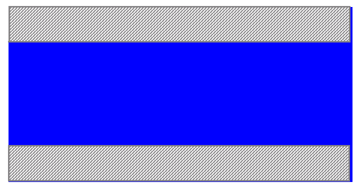
Flag	Description
ISDN_RESOURCE_POLICY (ISDN)	The flag value determines how the ISDN B-channels within configured spans are allocated. The robustness of the ISDN network can be improved by allocating channels evenly (load balancing) among the spans, minimizing the effect of channel loss resulting from the malfunction of a single span. Set the flag value to: • **LOAD_BALANCE** to allocate channels evenly among all configured spans. • **FILL_FROM_FIRST_CONFIGURED_SPAN** To allocate all channels on the first configured span before allocating channels on other spans. • **FILL_FROM_LAST_CONFIGURED_SPAN** To allocate all channels on the last configured span before allocating channels on other spans. Default: LOAD_BALANCE

Table 22-1 System Flags – MCMS_PARAMETERS (Continued)

<table>
<tr><th>Flag</th><th>Description</th></tr>
<tr><td>ITP_CROPPING</td><td>If the conference is set to TelePresence mode, cropping of the image is done according to this flag value:

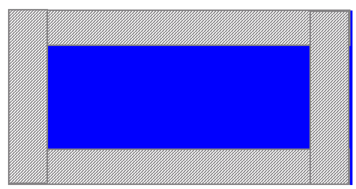
ITP (default) - Cropping is done as follows:

Left/right sides: no cropping
Top/Bottom: the calculated area to be stripped will be split and cropped equally from the top and the bottom of the display area.



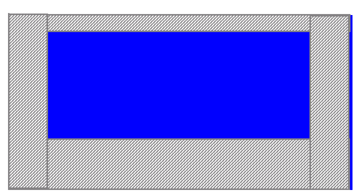
CP - Cropping is done as follows:

Left/right sides: the calculated area to be stripped will be split and cropped equally from the top and bottom of the image
Top/Bottom: the calculated area to be stripped will be split and cropped equally from both sides.



MIXED - Cropping is done as follows:

Left/right sides: the calculated area to be stripped will be split and cropped equally from the top and bottom of the image
Top/Bottom: the calculated area to be stripped will be cropped 84% of the calculated area to be stripped will be cropped from the bottom, and 16%will be cropped from the top.



Note: If the flag was added with no value, and the conference is set to TelePresence mode, cropping is done as follows:

Left/right sides: no cropping
Top/Bottom: the calculated area to be stripped will be cropped 84% of the calculated area to be stripped will be cropped from the bottom, and 16%will be cropped from the top.

</td></tr>
</table>

Table 22-1 System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
IVR_MESSAGE_VOLUME	The volume of IVR messages varies according to the value of this flag. Possible value range: 0-10 (Default: 6). 0 – disables playing the IVR messages 1 – lowest volume 10 – highest volume **Notes:** • It is not recommended to disable IVR messages by setting the flag value to 0. • System reset is not required for flag changes to take effect.
IVR_MUSIC_VOLUME	The volume of the IVR music played when a single participant is connected to the conference varies according to the value of this flag. Possible value range: 0-10 (Default: 5). 0 – disables playing the music 1 – lowest volume 10 – highest volume **Note:** System reset is not required for flag changes to take effect.
IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE	This flag is applicable in versions **prior** to version 7.6. In version 7.6 this flag is replaced by IVR Service - Roll Call/ Notifications options. When set to **YES**, the system does not playback the Roll Call names when participants enter or exit the conference. If the voice messages are replaced with tones the system will play these tones instead. The use of tones requires the uploading of the appropriate tone files in *wav format and replacing the *Roll Call Joined* and *Roll Call Left* message files with the tone files in the *Conference IVR Service - Roll Call* dialog box. When the flag is set to **NO**, Roll Call names are announced when participants enter or exit the conference. Default: NO.
IVR_ROLL_CALL_VOLUME	The volume of the Roll Call varies according to the value of this flag. Possible value range: 0-10 (Default: 6). 0 – disables playing the Roll Call 1 – lowest volume 10 – highest volume **Note:** • It is not recommended to disable the Roll Call by setting the flag value to 0. • System reset is not required for flag changes to take effect.

Table 22-1 System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
LAST_LOGIN_ATTEMPTS	If YES, the system displays a record of the last Login of the user. Default: NO. For more details, see "*User Login Record"* on page **15-13**.
LEGACY_EP_CONTENT_DEFAULT_LAYOUT	Defines the video layout to be displayed on the screen of the legacy endpoints when switching to Content mode. Default value: **CP_LAYOUT_1P7** (1+7). For a detailed list of possible flag values for the various video layouts, see Table 22-6, "*LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values,"* on page **22-43**.
MAX_CONF_PASSWORD_REPEATED_CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters that are to be allowed in a conference password. Range: 1 - 4 Default: 2 **Note:** In Version 7.7, if a Polycom DMA system is installed in your environment, you must change the value of this flag to **4** to maintain the compatibility between the RMX and the DMA.
MAX_CP_RESOLUTION	The MAX_CP_RESOLUTION flag value is applied to the system during *First Time Power-on* and after a system upgrade. The default value is HD1080. All subsequent changes to the Maximum CP Resolution of the system are made using the *Resolution Configuration* dialog box. Possible flag values: • **HD1080** – High Definition at 60 fps (MPM+ / MPMx) • **HD720** – High Definition at 60 fps (MPM+ / MPMx) • **HD** – High Definition at 30 fps • **SD30** – Standard Definition at 30 fps • **SD15** – Standard Definition at 15 fps • **CIF** – CIF resolution Default: HD1080 For more information see "*Video Resolutions in AVC-based CP Conferencing"* on page **3-1**.
*MAX_INTRA_REQUESTS_PER_INTERVAL_*	Enter the maximum number of refresh (intra) requests for the Content channel sent by the participant's endpoint in a 10 seconds interval that will be dealt by the RMX system. When this number is exceeded, the Content sent by this participant will be identified as noisy and his/her requests to refresh the Content display will be suspended. Default setting: 3
*MAX_INTRA_SUPPRESSION_DURATION_IN_SECONDS_*	Enter the duration in seconds to ignore the participant's requests to refresh the Content display. Default setting: 10

Table 22-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM	Defines the maximum number of concurrent management sessions (http and https connections) per system. Value: 4 - 80 Default: 80
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER	Defines the maximum number of concurrent management sessions (http and https connections) per user. Value: 4 - 80 Default: 10 (20 in Ultra Secure Mode)
MAX_PASSWORD_REPEATED_CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a password. Range: 1 - 4 Default: 2
MCU_DISPLAY_NAME	The name of the MCU that is displayed on the endpoint's screen when connecting to the conference. Default: POLYCOM RMX 1500/POLYCOM RMX 2000/ POLYCOM RMX 4000 depending on the product type.
MIN_PASSWORD_LENGTH	The length of passwords. Possible value: between 0 and 20. **0** means this rule is not enforced, however this rule cannot be disabled when the RMX is in Ultra Secure Mode. In Ultra Secure Mode, passwords must be at least 15 characters in length (default) and can be up to 20 characters in length. For more details, see "*Password Length"* on page **15-10**.
MIN_PWD_CHANGE_FREQUENCY_IN_DAYS	Defines the frequency with which a user can change a password. Values: 0 -7. **0** (standard default) - users do not have to change their passwords. In *Ultra Secure Mode* the retention period is between 1 (default) and 7. For details, see "*Defining Password Change Frequency"* on page **15-12**.
MIN_SYSTEM_DISK_SPACE_TO_ALERT	Defines a minimum remaining RMX disk capacity in megabytes. If the remaining RMX disk capacity falls below this level an active alarm is raised. **Default:** 2048

Table 22-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
MIN_TIP_COMPATIBILITY_LINE_RATE	This flag determines the minimum line rate at which conferencing entities such as an Entry Queue or Meeting Room can be TIP-enabled and TIP-enabled endpoints can connect to them. CTS version 7 requires a minimum line rate of 1024 kbps and will reject calls at lower line rates, therefore the System Flag value should be 1024 kbps or higher. **0** means that no minimum line rate is enforced on the conference for TIP connectivity. Default: 1024
MS_ENVIRONMENT	If YES, sets the RMX SIP environment to integrate with Microsoft OCS solution. Default: NO
MULTIPLE_SERVICES	Determines whether the Multiple Services option is be activated once the appropriate license is installed. Possible Values: YES / NO Default: NO **Note:** If the MULTIPLE_SERVICES System Flag is set to YES and no RTM ISDN or RTM LAN card is installed in the RealPresence Collaboration Server (RMX) 2000, an Active Alarm is displayed.
NUM_OF_LOWER_CASE_ALPHABETIC	The minimum number of lower case alphabetic characters required in a Login password in Ultra Secure Mode. Default: 0
NUM_OF_NUMERIC	The minimum number of numeric characters required in a Login password in Ultra Secure Mode. Default: 0
NUM_OF_SPECIAL_CHAR	The minimum number of special characters (asterisks, brackets, periods etc.) required in a Login password in Ultra Secure Mode. Default: 0
NUM_OF_UPPER_CASE_ALPHABETIC	The minimum number of upper case alphabetic characters required in a Login password in Ultra Secure Mode. Default: 0

Table 22-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
NUMERIC_CHAIR_PASS_DEFAULT_LEN	This flag enables or disables the automatic generation of chairperson passwords and determines the number of digits in the chairperson passwords assigned by the MCU. Possible values are: • **0** disables the automatic password generation in both Standard Security Mode or Ultra Secure Mode. Any value other than 0 enables the automatic generation of chairperson passwords if the flag HIDE_CONFERENCE_PASSWORD is set to NO. • **1 – 16**, default: 6 (Standard Security Mode) • **9 – 16**, default: 9 (Ultra Secure Mode). If the default is used, in non-secured mode the system will automatically generate chairperson passwords that contain 6 characters.
NUMERIC_CHAIR_PASS_MAX_LEN	The maximum number of digits that the user can enter when manually assigning a password to the chairperson. Range: • **0 – 16** (Standard Security Mode) • **9 – 16** (Ultra Secure Mode). Default (both Modes): 16
NUMERIC_CHAIR_PASS_MIN_LEN	Defines the minimum length required for the Chairperson password. Value: 0-16 Default: • **0** - (Standard Security Mode) this rule is not enforced. However this rules cannot be disabled when the RMX is in Ultra Secure Mode. • **9** - (*Ultra Secure Mode*) Chairperson password must be at least 9 characters in length (default).
NUMERIC_CONF_ID_LEN	Defines the number of digits in the Conference ID that will be assigned by the MCU. Enter 0 to disable the automatic assignment of IDs by the MCU and let the RMX user manually assign them. Range: 2-16 (Default: 4).
NUMERIC_CONF_ID_MAX_LEN	The maximum number of digits that the user can enter when manually assigning an ID to a conference. Range: 2-16 (Default: 8) **Note:** Selecting 2 limits the number of simultaneous ongoing conferences to 99.
NUMERIC_CONF_ID_MIN_LEN	The minimum number of digits that the user must enter when manually assigning an ID to a conference. Range: 2-16 (Default: 4) **Note:** Selecting 2 limits the number of simultaneous ongoing conferences to 99.

Table 22-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
NUMERIC_CONF_PASS_DEFAULT_LEN	This flag enables or disables the automatic generation of conference passwords and determines the number of digits in the conference passwords assigned by the MCU. Possible values are: • **0** disables the automatic password generation in both Standard Security Mode or Ultra Secure Mode. Any value other than 0 enables the automatic generation of conference passwords if the flag HIDE_CONFERENCE_PASSWORD is set to NO. • **1 – 16**, default: 6 (Standard Security Mode) • **9 – 16**, default: 9 (Ultra Secure Mode). If the default is used, in non-secured mode the system will automatically generate conference passwords that contain 6 characters.
NUMERIC_CONF_PASS_MAX_LEN	The maximum number of digits that the user can enter when manually assigning a password to the conference. Range: • **0 – 16** (Standard Security Mode) • **9 – 16** (Ultra Secure Mode). Default (both Modes): 16
NUMERIC_CONF_PASS_MIN_LEN	Defines the minimum length required for the Conference password. Value: 0-16 Default: • **0** - (Standard Security Mode) this rule is not enforced. However this rules cannot be disabled when the RMX is in Ultra Secure Mode. • **9** - (*Ultra Secure Mode*) Conference password must be at least 9 characters in length (default).
PAL_NTSC_VIDEO_OUTPUT	When set to AUTO (default), the video output sent by the RMX is either PAL or NTSC format, depending on the current speaker in the layout. This ensures full synchronization between the frame rate of the speaker and the video encoder, ensuring smoother video. In environments where the majority of endpoints are configured to either NTSC or PAL, the flag can be set accordingly to change the video encoding of the RMX to be compatible with the majority of endpoints in the call. Possible Values: AUTO, PAL, NTSC
PASSWORD_EXPIRATION_DAYS	Determines the duration of password validity. Value: between 0 and 90 days. 0 - user passwords do not expire. In *Ultra Secure Mode*: default - 60 days, the minimum duration is 7 days. For details, see "*Defining Password Aging"* on page **15-11**.

***Table 22-1** System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
PASSWORD_EXPIRATION_DAYS_MACHINE	Enables the administrator to change the password expiration period of *Application-user*'s independently of regular users. Default: 365 (days).
PASSWORD_EXPIRATION_WARNING_DAYS	Determines the display of a warning to the user of the number of days until password expiration. Value: between 0 and 14 days. 0 - password expiry warnings are not displayed. In *Ultra Secure Mode*, the earliest display - 14 days, the latest 7 days (default). For details, see "*Defining Password Aging"* on page **15-11**.
PASSWORD_HISTORY_SIZE	The number of passwords that are recorded to prevent users from re-using their previous passwords. Values are between 0 and 16. 0 (standard default) - the rule is not enforced, however this rule cannot be disabled when the RMX is in Ultra Secure Mode. In *Ultra Secure Mode*, at least 10 passwords (default) and up to 16 passwords must be retained. For more details, see "*Implementing Password Re-Use / History Rules"* on page **15-11**.
RESTRICT_CONTENT_BROADCAST_TO_LECTURER	If set to YES, only the conference lecturer may send content to the conference. If set to NO, any conference participant can send content. Default: YES
RMX2000_RTM_LAN	This flag is used after installation on and RTM-LAN card to activate the card. The flag must be set to YES. (RealPresence Collaboration Server (RMX) 2000 only.)
RRQ_WITHOUT_GRQ	To enable registration, some gatekeepers require sending first RRQ and not GRQ. Set flag to **YES**, if this behavior is required by the gatekeeper in your environment. Default: NO. *GRQ (Gatekeeper Request)* - Gatekeeper discovery is the process an endpoint uses to determine which gatekeeper to register with. *RRQ* - registration request sent to the gatekeeper.
SEPARATE_MANAGEMENT_NETWORK	Enables/disables the Network Separation. Can only be disabled in the Ultra Secure Mode (ULTRA_SECURE_MODE=YES). Default: NO.

Table 22-1 *System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
SESSION_TIMEOUT_IN_MINUTES	If there is no input from the user or if the connection is idle for longer than the number of minutes specified by this flag, the connection to the RMX is terminated. Value: 0-99 0 - Session Timeout is disabled, however this feature cannot be disabled when the RMX is in Ultra Secure Mode. Default: 0 Default (ULTRA_SECURE_MODE=YES): 10
SIP_AUTO_SUFFIX_EXTENSION	Used to automatically add a suffix to a SIP address (To Address) instead of adding it manually in the *RMX Web Client* (SIP address) when the SIP call is direct-dial and not through a Proxy. **Example:** Participant Name = john.smith Company Domain = maincorp.com SIP_AUTO_SUFFIX_EXTENSION flag value = @maincorp.com Entering john.smith will generate a SIP URI = john.smith@maincorp.com
SITE_NAMES_LOCATION (MPM+ Only)	In **MPM+ Mode** this flag is used to change the default location of the *Site Name* in the video layout. Default: DOWN CENTER = Bottom, centered Range: • UP_RIGHT = Top, right justified • UP_LEFT = Top, left justified • DOWN_RIGHT = Bottom, right justified • DOWN_LEFT = Bottom, left justified • UP_CENTER = Top, centered • DOWN_CENTER = Bottom, centered In **MPMx Mode** this function is controlled using the *Profile - Site Names* dialog box.
STAR_DELIMITER_ALLOWED	When set to YES, an asterisk “*” can be used as a delimiter in Conference and Meeting Room dial strings. The dial string is first searched for “'**#**' first followed by “*”. Default: NO
SYSTEM_BROADCAST_VOLUME	This value is used when the system flag FORCE_SYSTEM_BROADCAST_VOLUME is set to YES. Determines the default audio level with which the participants connects and sends audio to the conference. The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default connection value is 5. Each unit change represents an increase or decrease of 3 dB (decibel). Range: 1-10 Default: 5

Table 22-1 *System Flags – MCMS_PARAMETERS (Continued)*

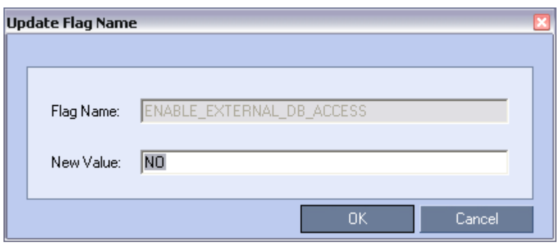
Flag	Description
SYSTEM_LISTENING_VOLUME	This value is used when the system flag FORCE_SYSTEM_LISTENING_VOLUME is set to YES. Determines the default audio level with which the participants connects and receives audio from the conference. The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default value is 5. Each unit change represents an increase or decrease of 3 dB (decibel). Range: 1-10 Default: 5
TERMINATE_CONF_AFTER_CHAIR_DROPPED	If YES, sets conferences to automatically terminate if the Chairperson disconnects from the conference. This takes effect only if the *Conference Requires Chairperson* check box in the Conference Profile Properties, IVR Tab, is selected. Default: YES **Note:** In order for the "Chairperson Exit" message to be played this flag must be set to YES.
ULTRA_SECURE_MODE	When set to YES enables the Ultra Secure Mode. When enabled, affects the ranges and defaults of the System Flags that control: • Network Security • User Management • Strong Passwords • Login and Session Management • Cyclic File Systems alarms Default: NO For a list of flags affected when the Ultra Secure Mode is enabled, see "*Auto Layout Configuration"* on page **22-41**.
USE_GK_PREFIX_FOR_PSTN_CALLS	When set to **YES** the *Gatekeeper Prefix* is included in the *DTMF* input string enabling *PSTN* participants to use the same input string when connecting to an RMX whether the RMX is a standalone MCU or part of a *DMA* solution deployment. Possible Values: YES / NO Default: NO For more information see "*PSTN Dial-in Using GK Prefix"* on page **19-9**.
USER_LOCKOUT	If YES, a user is locked out of the system after three consecutive Login failures with same User Name. The user is disabled and only the administrator can enable the user within the system. Default: NO Default in Ultra Secure Mode: YES For details, see "*User Lockout"* on page **15-12**.

Table 22-1 System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
USER_LOCKOUT_DURATION_IN_MINUTES	Defines the duration of the Lockout of the user. Value: 0 - 480 0 means permanent User Lockout until the administrator re-enables the user within the system. Default: 0
USER_LOCKOUT_WINDOW_IN_MINUTES	Defines the time period during which the three consecutive Login failures occur. Value: 0 - 45000 0 means that three consecutive Login failures in any time period will result in User Lockout. Default: 60

3 To modify a flag value, double-click or select the flag and click the **Edit Flag** button.

4 In the *New Value* field, enter the flag's new value.



5 Click **OK** to close the *Update Flag* dialog box.

6 Repeat steps 2–4 to modify additional flags.

7 Click **OK** to close the *System Flags* dialog box

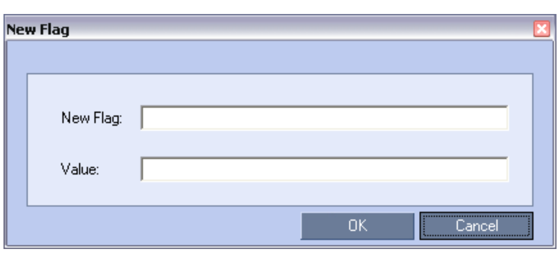
For flag changes (including deletion) to take effect, reset the MCU. For more information see "*Resetting the RMX"* on page **21-69**.

Manually Adding and Deleting System Flags

To add a flag:

1 In the *System Flags* dialog box, click the **New Flag** (
) button.

The *New Flag* dialog box is displayed.



2 In the *New Flag* field enter the flag name.

3 In the *Value* field enter the flag value.

The following flags can be manually added to the *MCMS_PARAMETERS* tab:

***Table 22-2** Manually Added System Flags – MCMS_PARAMETERS*

Flag	Description
ACCEPT_VOIP_DTMF_TYPE	Defines the type of *DTMF* tones *(inband)* or digits (*outband)* that the RMX will accept in *VOIP* calls. **Range:** • **0** - Auto (default): *Inband* or *outband DTMF* tones/digits are accepted depending on the endpoint's current setting. If the endpoint switches from *inband* to *outband* or visa versa the value of the SET_DTMF_SOURCE_DIFF_IN_SEC flag determines the time interval after which both *inband* and *outband* tones/digits will be accepted. • **1** - *Outband* (H.245) only • **2** - *Inband* only
ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF	If YES, allows non-encrypted participants to connect to encrypted conferences. Default: No **Note:** From Version 7.6.1, this flag is replaced by the Encryption option “Encrypt when Possible” in the conference Profile - Advanced dialog box. Flag setting is ignored.
ALWAYS_FORWARD_DTMF_IN_GW_SESSION_TO_ISDN (ISDN)	When set to YES, all DTMF codes sent by participants in the GW session will be forwarded to all PSTN and ISDN participants in the same GW session. Range: YES / NO Default Value: NO
APACHE_KEEP_ALIVE_TIMEOUT	If the connection is idle for longer than the number of seconds specified by this flag, the connection to the RMX is terminated. Value: 0 - 999 Default: 120 Default (ULTRA_SECURE_MODE=YES): 15 **Note:** A value of 0 results in an unlimited keep-alive duration. This value should **never** be used in *Ultra Secure Mode*.
AVOID_VIDEO_LOOP_BACK_IN_CASCADE	When set to YES the current speaker’s image is not sent back through the participant link in cascaded conferences with conference layouts other than 1x1. Default: YES Range: YES / NO

Table 22-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
BONDING_DIALING_METHOD (ISDN)	When set to: • **SEQUENTIAL** The MCU initiates channel connections sequentially until it reaches the number of channels defined by the BONDING_NUM_CHANNELS_IN _GROUP flag. When a channel is connected, dialing begins for the next channel in the group. • **BY_TIMERS** The MCU initiates channel connections sequentially using the values of the BONDING_CHANNEL _DELAY and BONDING_GROUP_DELAY flags. The first group of channels is dialed, using the BONDING_CHANNEL_DELAY between dialing attempts for each channel in the group. The RMX then implements the BONDING_GROUP_DELAY, before dialing the first channel of the next group. Default: SEQUENTIAL
BONDING_GROUP_DELAY (ISDN)	When connecting several bonding groups, this is the delay (number of 1/100 seconds) preceding the first dialing attempt to connect the next bonding group. Default: 500
BONDING_NUM_CHANNELS_IN_GROUP (ISDN)	The number of channels in the bonding group to be connected before dialing the next sequential channel. Default: 50
BURN_BIOS	Although not recommended, setting this flag's value to NO will prevent BIOS upgrade. Default: YES.
CAC_ENABLE	When set to YES, enables the Call Admission Control implementation in the RMX. Default: NO (CAC is disabled)
CASCADE_LINK_PLAY_TONE_ON_CONNECTION	When set to **YES,** the RMX plays a tone when a cascading link between conferences is established. The tone is played in both conferences. This tone is not played when the cascading link disconnects from the conferences. The tone used to notify that the cascading link connection has been established cannot be customized. Default value: **NO**. The tone volume is controlled by the same flag as the IVR messages and tones: IVR_MESSAGE_VOLUME.

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
CELL_IND_LOCATION	Change the location of the display of *Network Quality Indicators* displayed in the cells of the conference *Video Layout*. Default: TOP_RIGHT Range: • BOTTOM_LEFT • BOTTOM_RIGHT • TOP_LEFT • TOP_RIGHT
CFG_KEY_ENABLE_FLOW_CONTROL_REINVITE	Used to enable or disable sending a *re-INVITE* to endpoints to adjust their data rate. When set to YES, *re*-INVITE is used for endpoints that do not support *flow control* in SIP using either the *Information* or *RTCP Feedback* mechanisms. Default: NO.
CONF_GATHERING_DURATION_SECONDS	The value of this *System Flag* sets the duration of the *Gathering Phase* in seconds. The *Gathering Phase* duration of the conference is measured from the scheduled start time of the conference. Range: 0 - 3600 Default: 180 For more information see "*Video Preview"* on page **4-26**.
CP_REGARD_TO_INCOMING_SETUP_RATE	For use in the Avaya Environment. If set to YES, the RMX calculates the line rate for incoming calls in CP conferences, according to the line rate which is declared by the endpoint in the H.225 setup message. If set to NO, the rate is calculated according to the conference line rate regardless of the rate in the H.225 setup message. Default: YES.
CPU_BONDING_LINK_MONITORING_FREQUENCY	Used when using the *MII Monitor* for troubleshooting networks.This flag sets the *MII Polling Interval* in milliseconds. A value of zero disables *MII* monitoring. Default: 100

***Table 22-2** Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
CPU_BONDING_MODE	Sets the *Bonding Mode* of the *Signalling* and *Management* network interface controllers. *Mode=6, balance-alb,* *(Adaptive Load Balancing)* includes *balance-tlb, (Transmit Load Balancing*) and *balance-rlb* (*Receive Load Balancing*) for *IPV4* traffic. No special switch support is required. *Receive Load Balancing* is achieved by *ARP* negotiation. Outbound ARP Replies are intercepted and their source hardware address is overwritten with the unique hardware address of one of the slaves in the bond. In this way different peers will use different hardware addresses for the server. **Note:** *balance-alb* is the only supported value. All other possible values are for troubleshooting purposes only. **Default:** *balance-alb* **Possible values:** • balance-alb • balance-rr • active-backup • balance-xor • broadcast • 802.3ad • balance-tlb
DELAY_BETWEEN_H320_DIAL_OUT_PARTY (ISDN)	The delay in milliseconds that the MCU waits when connecting dial out ISDN and PSTN participants. Default: 1000
DISABLE_CELLS_NETWORK_IND	Disable the display of *Network Quality Indicators* displayed in the cells of the conference *Video Layout*. Default: YES Range: YES / NO
DISABLE_DUMMY_REGISTRATION	Enables or disables SIP dummy registration on the domain. Possible Values: NO (Default) - Disables SIP dummy registration. YES - Enables SIP dummy registration. **Note:** For homologation and certification testing, the flag must be set to YES.
DISABLE_GW_OVERLAY_INDICATION	When set to **NO** (default), displays progress indication during the connection phase of a gateway call. Set the value to **YES** to hide the connection indications displayed on the participant's screen during the connection phase of a gateway call.
DISABLE_SELF_NETWORK_IND	Disable the display of the *Network Quality Indicator* of the participant's own endpoint. Default: NO Range: YES / NO

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
DISABLE_WIDE_RES_TO_SIP_DIAL_OUT	When set to **NO** (default), the RMX sends wide screen resolution to dial-out SIP endpoints. Endpoint types that do not support wide screen resolutions are automatically identified by the RMX according to their product type and version and will not receive the wide resolution even if the flag is set to YES. When manually added and set to **YES**, the RMX does not send wide screen. Default: NO.
DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS	Used for DTMF code suppression in cascading conferences. Determines the time period (in seconds) that MCU A will forward DTMF inputs from conference A participants to MCU B. Flag range (in seconds): 0 - 360000 This flag is defined on MCU A (the calling MCU). For more information, see "*Suppression of DTMF Forwarding”* on page **5-13**.
ENABLE_1080_SVC	When set to YES *HD1080p30* is enabled as the highest supported resolution in *SVC* mode. **Range:** YES / NO **Default:** NO
ENABLE_CISCO_GK	When set to YES, it enables the use of an identical prefix for different RMXs when registering with a Cisco MCM Gatekeeper. Default: NO.
ENABLE_CLOSED_CAPTION	Enables or disables the Closed Captions option that allow endpoints to endpoints to provide real-time text transcriptions or language translations of the video conference. When set to NO (default), Closed Captions are disabled. When set to YES, Closed Captions are enabled.
ENABLE_EPC	When set to YES (default), enables Polycom proprietary People+. When set to NO, disables this feature for all conferences and participants.
ENABLE_EXTERNAL_DB_ACCESS	If YES, the RMX connects to an external database application, to validate the participant’s right to start a new conference or access a conference. Default: NO

Table 22-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
ENABLE_H239	When set to YES, Content is sent via a separate Content channel. Endpoints that do not support H.239 Content sharing will not be able to receive When set to NO, the Content channel is closed. In such a case, H.239 Content is sent via the video channel (“people” video) enabling endpoints that do not support H.239 Content sharing to receive the Content in their video channel. Default: YES.
ENABLE_H239_ANNEX_T	In H.239-enabled MIH Cascading, when MGC is on level 1, enables sending Content using Annex T.
ENABLE_IP_REDIAL	In all versions up to version 7.0, when set to YES (default), it enables re-dialing if H.323 or SIP dial out calls fail. In version 7.0 and later, this flag functionality is replaced by the **Auto Redialing** check box in the *Profile Properties - Advanced* dialog box
ENABLE_LYNC_RTCP_INTRA	When set to YES, *RTCP FIR* is used for sending *Intra Requests*. When set to NO *Intra Requests* are sent using *SIP INFO Messages*. **Range:** YES / NO **Default:** NO
ENABLE_MS_FEC	Enables the Microsoft FEC (Forward Error Correction) support for RTV. Range: Auto/No Default: Auto When set to **Auto**, FEC support is enabled. FEC uses the DV00 option (DV=00 - one FEC per frame using XOR). When set to **No**, FEC support is disabled.
ENABLE_NO_VIDEO_RESOURCES_AUDIO_ONLY_MESSAGE	Enables playing a voice message that Informs the participant of the lack of Video Resources in the RMX and that he/she is being connected as Audio Only. Default: YES
ENABLE_SIP_PEOPLE_PLUS_CONTENT	If security is of higher priority than SIP Content sharing, SIP People+Content can be disabled by setting this System Flag to NO. (The content management control (BFCP) utilizes an unsecured channel (60002/TCP) even when SIP TLS is enabled.) Default: YES
ENABLE_SIP_PPC_FOR_ALL_USER_AGENT	When set to YES, SIP People+Content and BFCP capabilities are declared with all vendors’ endpoints. Default: YES Range: YES / NO
ENABLE_SIRENLPR	Enable / disable SirenLPR Audio Algorithm for use in IP (H.323, SIP) calls in both CP and VSW conferences. Range: YES / NO Default: YES

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
ENABLE_SIRENLPR_SIP_ENCRYPTION	Enables the *SirenLPR* audio algorithm when using encryption with the *SIP* protocol. Range: YES / NO Default: NO
ENABLE_TC_PACKAGE	Enables or disables Network Traffic Control. Range: YES / NO Default: NO
ENABLE_TEXTUAL_CONFERENCE_STATUS	Set the value of this flag to NO to disable *Text Indication.* This setting is recommended for MCUs running Telepresence conferences. Default: YES.
ENABLE_VIDEO_PREVIEW	Enables the Video Preview feature. Default: YES. For more details, see "*Video Preview"* on page **4-26**.
EXTERNAL_CONTENT_DIRECTORY	The Web Server folder name. Change this name if you have changed the default names used by the CMA application. Default: /PlcmWebServices
EXTERNAL_CONTENT_IP	**Version 4.x and earlier -** enter the IP address of the CMA server. **Version 5.0** - enter the IP address of the CMA server in the format: **http://[IP address of the CMA server]**. For example, http://172.22.185.89. This flag is also the trigger for replacing the internal RMX address book with the CMA global Address Book. When empty, the integration of the CMA address book with the RMX is disabled.
EXTERNAL_CONTENT_PASSWORD	The password associated with the user name defined for the RMX in the CMA server.
EXTERNAL_CONTENT_PORT	The CMA port used by the RMX to send and receive XML requests/responses. Default: 80.
EXTERNAL_CONTENT_USER	The login name defined for the RMX in the CMA server defined in the format: domain name/user name.
EXTERNAL_DB_DIRECTORY	The URL of the external database application. For the sample script application, the URL is: *<virtual directory>/SubmitQuery.asp*
EXTERNAL_DB_IP	The IP address of the external database server, if one is used. Default: 0.0.0.0
EXTERNAL_DB_LOGIN	The login name defined for the RMX in the external database server. Default: POLYCOM

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
EXTERNAL_DB_PASSWORD	The password associated with the user name defined for the RMX on the external database server. Default: POLYCOM
EXTERNAL_DB_PORT	The external database server port used by the RMX to send and receive XML requests/responses. For secure communications set the value to 443. Default: 5005.
FADE_IN_FADE_OUT	Enables or disables the transition format between speakers in a Continuous Presence conference. When set to YES (default), the system fades in the current speaker while fading out the previous speaker. When set to NO, the transition is sharp and immediate. **Note:** *Fade In / Fade Out* is not supported with *MPMx* cards.
FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION	When set to **YES**, the cascaded link is automatically set to Full Screen (1x1) in CP conferences forcing the speaker in one cascaded conference to display in full window in the video layout of the other conference. Set this flag to **NO** when connecting to an MGC using a cascaded link, if the MGC is functioning as a Gateway and participant layouts on the other network are not to be forced to 1X1. Default: YES
FORCE_AUDIO_CODEC_FOR_MS_SINGLE_CORE	This flag is used to force the use of a specific Audio algorithm when a Microsoft Office Communicator R2 or Lync Client is hosted on a workstation with a single core processor. The flag value overrides the default audio algorithm selection (G.722.1) that may cause audio quality problems when G.722.1 is used by Microsoft Clients running on single processor workstations. This flag can be set to: • **AUTO** – No forcing occurs and the RMX negotiates a full set of Audio algorithm during capabilities exchange. • **G711A/U** or **G722** – Set this flag value according to the hosting workstation capabilities. If the RMX detects single core host during capabilities exchange it will assign a G.711 or G.722 Audio algorithm according to the flag value. Possible values: AUTO, G711A, G711U, G722 Default: G711A
FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE	When set to **YES** (default), *Undefined participants* must connect encrypted, otherwise they are disconnected. When set to **NO** and the conference *Encryption* in the *Profile* is set to “Encrypt When Possible”, both Encrypted and Non-encrypted *Undefined participants* can connect to the same conferences, where encryption is the preferred setting. Default: YES

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
FORCE_G711A	Setting this flag forces the use of the *G711A Audio Codec.* **Possible values:** YES / NO **Default:** NO
FORCE_RESOLUTION	Use this flag to specify IP (H.323 and SIP) endpoint types that cannot receive wide screen resolution and that were not automatically identified as such by the RMX. Possible values are endpoint types, each type followed by a semicolon. For example, when disabling Wide screen resolution in an HDX endpoint enter the following string: **HDX;** **Note:** Use this flag when the flag SEND_WIDE_RES_TO_IP is set to YES.
FORCE_STATIC_MB_ENCODING	This flag supports Tandberg MXP mode of sending and receiving video by IP endpoint in HD 720p resolution and Video Quality set to Motion. This mode is not supported for ISDN endpoints. Default value: **Tandberg MXP**. To disable this flag, enter **NONE**.
G728_IP	Enables or disables declaration of G.728 Audio Algorithm capabilities in IP calls. Range: YES / NO Default: NO
G728_ISDN	Enables or disables declaration of G.728 Audio Algorithm capabilities in ISDN calls. Range: YES / NO Default: NO
H239_FORCE_CAPABILITIES	When the flag is set to NO, the RMX only verifies that the endpoint supports the Content protocols: Up to H.264 or H.263. When set to YES, the RMX checks frame rate, resolution and all other parameters of the Content mode as declared by an endpoint before receiving or transmitting Content. Default: NO.
H264_BASE_PROFILE_MIN_RATE_CIF60_MOTION	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for CIF60 resolution using Motion Video Quality. Default: 256kbps
H264_BASE_PROFILE_MIN_RATE_HD1080P30_SHARPNESS	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for HD1080P30 resolution using Sharpness Video Quality. Default: 1536kbps

Table 22-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
H264_BASE_PROFILE_MIN_RATE_HD720P30_SHARPNESS	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for HD720P30 resolution using Sharpness Video Quality. Default: 1024kbps
H264_BASE_PROFILE_MIN_RATE_HD720P60_MOTION	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for HD720P60 resolution using Motion Video Quality. Default: 1536kbps
H264_BASE_PROFILE_MIN_RATE_SD30_SHARPNESS	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for SD30 resolution using Sharpness Video Quality. Default: 256kbps
H264_BASE_PROFILE_MIN_RATE_SD60_MOTION	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for SD60 resolution using Motion Video Quality. Default: 1024kbps
H264_HD_GRAPHICS_MIN_CONTENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high quality content via the Content channel When Content Setting is Graphics. Range: 0-1536 Default: 128
H264_HD_HIGHRES_MIN_CONTENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high quality content via the Content channel When Content Setting is Hi Resolution Graphics. Range: 0-1536 Default: 256
H264_HD_LIVEVIDEO_MIN_CONTENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high quality content via the Content channel When Content Setting is Live Video. Range: 0-1536 Default: 384
H323_FREE_VIDEO_RESOURCES	For use in the Avaya Environment. In the Avaya Environment there are features that involve converting undefined dial-in participants' connections from video to audio (or vice versa). To ensure that the participants' video resources remain available for them, and are not released for use by Audio Only calls, set this flag to **NO**. If set to YES, the RMX will release video resources for *Audio Only* calls. Default: YES.

Table 22-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description

HIDE_CONFERENCE_PASSWORD	If set to YES (default in Ultra Secure Mode):
	• Conference and Chairperson Passwords that are displayed in the *RMX Web Client* or *RMX Manager* are hidden when viewing the properties of the conference.
	• Automatic generation of passwords (both conference and chairperson passwords) is disabled, regardless of the settings of the flags:
	  • NUMERIC_CONF_PASS_DEFAULT _LEN
	  • NUMERIC_CHAIR_PASS_ DEFAULT_LEN.
	For more information see "*Automatic Password Generation Flags"* on page **22-45**
	Default: NO.

IP_LINK_ENVIRONMENT	In H.239-enabled MIH Cascading, when MGC is on level 1, setting this flag to YES will adjust the line rate of HD Video Switching conferences run on the RMX 1500/2000/4000 from 1920Kbps to 18432, 100bits/sec to match the actual rate of the IP Only HD Video Switching conference running on the MGC. **Note:** If the flag MIX_LINK_ENVIRONMENT is set to NO, the *IP_ENVIRONMENT_LINK* flag must be set to YES.
IP_RESPONSE_ECHO	When the *System Flag* value is **YES**, the RMX will respond to *ping (IPv4)* and *ping6 (IPv6)* commands. When set to **NO**, the RMX will not respond to *ping* and *ping6* commands.
ITP_CERTIFICATION	When set to **NO** (default), this flag disables the telepresence features in the Conference Profile. Set the flag to **YES** to enable the telepresence features in the Conference Profile (provided that the appropriate License is installed).
LAN_REDUNDANCY	Enables Local Area Network port redundancy on RMX 2000/4000 RTM LAN Card and RealPresence Collaboration Server (RMX) 1500 LAN ports on the RTM IP 1500. Default: YES Range: YES / NO
MAX_ALLOWED_RTV_HD_FRAME_RATE	Defines the threshold Frame Rate (fps) in which RTV Video Protocol initiates HD resolutions. Flag values are as follows: Range: 0-30 (fps) Default: 0 (fps) - Implements any Frame Rate based on Lync RTV Client capabilities
MAX_RTV_RESOLUTION	Enables you to override the RMX resolution selection and limit it to a lower resolution, hence minimizing the resource usage to 1 or 1.5 video resources per call instead of 3 resources. Possible flag values are: AUTO (default), QCIF, CIF, VGA or HD720.

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
MAX_TRACE_LEVEL	This flag indicates the debugging level for RMX support. The flag's values have been modified for version 7.8 and is not backward compatible with previous versions. **Possible values:** From version 7.8 - TRACE = t, DEBUG = d, INFO_NORMAL = n, INFO_HIGH = i, WARN = w, ERROR = e, FATAL = f, OFF = o. From version 7.7 or lower - TRACE = n/a, DEBUG = n/a, INFO_NORMAL = n, INFO_HIGH = api, WARN = n/a, ERROR = crt, FATAL = n/a, OFF = no. **Default:** n
MAXIMUM_RECORDING_LINKS	The maximum number of Recording Links available for selection in the Recording Links list and the Conference Profile - Recording dialog box. Range: 1 - 100 Default: 20
MEDIA_NIC_MTU_SIZE	MTU size (Maximum Transmission Unit controls the maximum data payload size (bytes) transmitted in a single packet over the network. The RMX sends large amount of data over the network and may be required to adjust its MTU size according to the network environment in which it is deployed. MTU configuration is applicable to RMXs with RTM-LAN cards installed only. Default: 1500
MIN_H239_HD1080_RATE	Used to set the threshold line rate for HD Resolution Content : the line rate at which the RMX will send Content at HD1080 Resolution. Setting the flag to 0 disables HD Resolution Content. Default: 768 kbps.
MINIMUM_FRAME_RATE_THRESHOLD_FOR_SD	Low quality, low frame rate video is prevented from being sent to endpoints by ensuring that an SD channel is not opened at frame rates below the specified value. Range: 0 -30 Default: 15
MIX_LINK_ENVIRONMENT	In H.239-enabled MIH Cascading, when MGC is on level 1, setting this flag to YES will adjust the line rate of HD Video Switching conferences run on the RMX 1500/2000/4000 from 1920Kbps to 17897, 100bits/sec to match the actual rate of the HD Video Switching conference running on the MGC. **Note:** If the flag MIX_LINK_ENVIRONMENT is set to YES, the IP_ENVIRONMENT_LINK flag must be set to NO.

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
MS_CAC_AUDIO_MIN_BR	The minimum bit rate for audio using the Microsoft CAC (Call Admission Control) protocol. When the bit rate is lower than the MS_CAC_AUDIO_MIN_BR, the call is not connected. Range: 0 - 384 Default: 30
MS_CAC_VTDEO_MIN_BR	The minimum bit rate for video using the Microsoft CAC (Call Admission Control) protocol. When the bit rate is lower than the MS_CAC_VIDEO_MIN_BR, the call is not connected as a video call.. Range: 0 - 384 Default: 40
MS_KEEP_ALIVE_ENABLE	Enables the Microsoft keep alive flag. Set it **YES** to ensure that endpoints such as HDX remain connected to the conference for its duration when the RMX is configured with FQDN address and the Lync server is working with load balancing and holds more than one address. Range: YES/NO Default: NO
MS_PROXY_REPLACE	Enables the *proxy=replace* parameter in the *SIP Header*. When set to YES the outbound proxy to replaces the contact information in the contact header with its own enabling other clients and servers to reach the client using the proxy's *IP* address, even if the client is behind a firewall. **Possible Values:** YES / NO **Default:** YES
NETWORK_IND_CRITICAL_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from *Major* to *Critical*. Default: 5
NETWORK_IND_MAJOR_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from *Normal* to *Major*. Default: 1
NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT	Indicates how many times the Hello (keep alive) message is sent from the RMX to the endpoint in an environment that includes a Session Border Controller (SBC) with a 3-second interval between messages. Range: 1 to 10. Default:3
NUMBER_OF_REDIAL	Enter the number re dialing attempts required. Dialing may continue until the conference is terminated. Default: 3

Table 22-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
PARTY_GATHERING_DURATION_SECONDS	The value of this *System Flag* sets the duration, in seconds, of the display of the *Gathering* slide for participants that connect to the conference after the conference start time. Range: 0 - 3600 Default: 15 For more information see "*Video Preview"* on page **4-26**.
PASSWORD_FAILURE_LIMIT	The number of unsuccessful Logins permitted in Ultra Secure Mode. Default: 3
PCM_FECC	Determines whether the DTMF Code, ##, the Far/Arrow Keys (FECC) or both will activate the PCM interface. This flag can be also be used in combination with DTMF code definitions to disable PCM. Possible Values: YES / NO Default: YES.
PCM_LANGUAGE	Determines the language of the PCM interface. Possible Values are: ENGLISH, CHINESE_SIMPLIFIED, CHINESE_TRADITIONAL, JAPANESE, GERMAN, FRENCH, SPANISH, KOREAN, PORTUGUESE, ITALIAN, RUSSIAN, NORWEGIAN Default: Current RMX Web Client language.
PORT_GAUGE_ALARM	When set to YES, if system resource usage reaches the High Port Usage Threshold as defined for the Port Gauges, System Alerts in the form of an Active Alarm and an SNMP trap are generated.
PRESERVE_ICE_CHANNEL_IN_CASE_OF_LOCAL_MODE	When set to NO (default), local the ICE channel is closed after applying CAC bandwidth management when Call Admission Control is enabled in the local network. When set to YES, the ICE channel is preserved open throughout the call. Default: NO
PSTN_RINGING_DURATION_SECONDS	If there is a slow response from the *ISDN* switch, the *PSTN* dial-out ringing duration (in seconds) is used by the RMX to disconnect the call. Default: 45
QOS_IP_AUDIO	Used to select the priority of audio packets when *DiffServ is* the is the selected method for packet priority encoding. Default: 0x88
QOS_IP_VIDEO	Used to select the priority of video packets when *DiffServ is* the is the selected method for packet priority encoding. Default: 0x88
REDIAL_INTERVAL_IN_SECONDS	Enter the number of seconds that the RMX should wait before successive re dialing attempts. Range: 0-30 (Default: 10)

Table 22-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
REMOVE_H323_EPC_CAP_TO_NON_POLYCOM_VENDOR	Used to disable *EPC* protocol. Use of *Polycom's* proprietary protocol, *High Profile*, *EPC*, may result in interoperability issues when used with other vendors' endpoints. **Possible values:** YES / NO **Default:** NO
REMOVE_H323_HIGH_PROFILE_CAP_TO_NON_POLYCOM_VENDOR	Used to disable *High Profile* protocol. Use of *Polycom's* proprietary protocol, *High Profile*, may result in interoperability issues when used with other vendors' endpoints. **Possible values:** YES / NO **Default:** NO
REMOVE_H323_HIGH_QUALITY_AUDIO_CAP_TO_NON_POLYCOM_VENDOR	Used to disable the following *Audio Codecs*: • G231 • G7221C • G7221 • G719 • Siren22 • Siren14 **Possible values:** YES / NO **Default:** NO
REMOVE_H323_LPR_CAP_TO_NON_POLYCOM_VENDOR	Used to disable *H.323 LPR* protocol. Use of *Polycom's* proprietary protocol, *H.323 LPR*, may result in interoperability issues when used with other vendors' endpoints. **Possible values:** YES / NO **Default:** NO
RMX_MANAGEMENT_SECURITY_PROTOCOL	Enter the protocol to be used for secure communications. Default: TLSV1_SSLV3 (both). Default for U.S. Federal licenses: TLSV1.
RTCP_FIR_ENABLE	When set to YES, the *Full Intra Request* (*FIR*) is sent as *INFO* (and not *RTCP*). Default = YES
RTCP_FLOW_CONTROL_TMMBR_ENABLE	Enables/disables the SIP RTCP flow control parameter. Default: YES
RTCP_FLOW_CONTROL_TMMBR_INTERVAL	Modifies the interval (in seconds) of the TMMBR (Temporary Maximum Media Stream Bit Rate) parameter for SIP RTCP flow control. Range: 5 - 999 (seconds) Default: 180
RTCP_PLI_ENABLE	When set to YES, the (Picture Loss Indication (*PLI*) is sent as *INFO* (and not *RTCP*). Default = YES

***Table 22-2** Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
SELF_IND_LOCATION	Change the location of the display of the *Network Quality Indicator* of the participant's own endpoint. Default: BOTTOM_RIGHT Range: • TOP_ LEFT • TOP • TOP_RIGHT • BOTTOM_ LEFT • BOTTOM • BOTTOM_RIGHT
SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD	When set to **YES**, it enables the RMX to send a busy notification to a SIP audio endpoint or a SIP device when dialing in to the RMX whose audio resource usage exceeded the Port Usage threshold. When set to **NO**, the system does limit the SIP audio endpoint connections to a certain capacity and will not send a busy notification when the resource capacity threshold is exceeded. Default: NO
SEND_SRTP_MKI	Enables or disables the inclusion of the *MKI* field in *SRTP* packets sent by the RMX. Set the value to NO to disable the inclusion of the *MKI* field in *SRTP* packets sent by the RMX when using endpoints (eg. *CounterPath Bria 3.2 Softphone*) that cannot decrypt *SRTP*-based audio and video streams if the *MKI* (*Master Key Identifier*) field is included in *SRTP* packets sent by the RMX. **Notes:** • This *System Flag* must be set to YES (default) when *HDX* endpoints, *Microsoft Office Communicator* and *Lync Clients* are used as they all support *SRTP* with *MKI*. • The system flag must be added and set to NO when Siemens phones (Openstage and ODC WE) are used in the environment as they do not support *SRTP* with *MKI*. Default: YES
SEND_WIDE_RES_TO_IP	When set to **YES** (default), the RMX sends wide screen resolution to IP endpoints. Endpoint types that do not support wide screen resolutions are automatically identified by the RMX according to their product type and version and will not receive the wide resolution even when the flag is set to YES. When manually added and set to **NO**, the RMX does not send wide screen resolution to all IP endpoints. Default: YES.

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
SEND_WIDE_RES_TO_ISDN	When set to **YES**, the RMX sends wide screen resolution to ISDN endpoints. When set to **NO** (default), the RMX does not send wide screen resolution to ISDN endpoints. Default: NO.
SET_AUDIO_CLARITY	*Audio Clarity* improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity. The enhancement is applied to the following low bandwidth (4kHz) audio algorithms: • G.729a • G.711 • Guidelines **Note:** This flag sets the initial value for *Audio Clarity* during *First-time Power-up*. Thereafter the feature is controlled via the *New Profile - Audio Settings* dialog box. *Audio Clarity* is supported with *MPM+* cards only Possible Values: ON / OFF Default: OFF For more information see "*Defining New Profiles"* on page **2-18**.
SET_AUDIO_PLC	*Packet Loss Concealment* (*PLC*) for Siren audio algorithms improves received audio when packet loss occurs in the network. The following audio algorithms are supported: • Siren 7 (mono) • Siren 14 (mono/stereo) • Siren 22 (mono/stereo) **Note:** *PLC for Audio* is supported with *MPM+ / MPMx* cards only. The speaker's endpoint must use a *Siren* algorithm for audio compression. Possible Values: ON / OFF Default: ON
SET_AUTO_BRIGHTNESS	*Auto Brightness* detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout. *Auto Brightness* only increases brightness and does not darken video windows. **Note:** This flag sets the initial value for *Auto Brightness* during *First-time Power-up*. Thereafter the feature is controlled via the *New Profile - Video Quality* dialog box. *Auto Brightness* is supported with *MPM+ / MPMx* cards only. Possible Values: YES / NO Default: NO For more information see "*Defining New Profiles"* on page **2-18**.

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
SET_DTMF_SOURCE_DIFF_IN_SEC	If the ACCEPT_VOIP_DTMF_TYPE flag is set to 0 (Auto) this flag determines the interval, in seconds after which the RMX will accept both *DTMF* tones *(inband)* and digits (*outband)*. **Default:** 120
SIP_BFCP_DIAL_OUT_MODE	Controls *BFCP's* use of *UDP* and *TCP* protocols for dial-out *SIP Client* connections according to its value: • **AUTO** (Default) *If SIP Client* supports *UDP, TCP* or *UDP* and *TCP*: - BFCP/UDP is selected as *Content* sharing protocol. • **UDP** *If SIP Client* supports *UDP* or UDP and TCP: - *BFCP/UDP* selected as *Content* sharing protocol. *If SIP Client* supports *TCP* - Cannot share *Content*. • **TCP** *If SIP Client* supports *TCP* or *UDP* and *TCP* - BFCP/TCP selected as Content sharing protocol. *If SIP Client* supports UDP - Cannot share Content.
SIP_DUAL_DIRECTION_TCP_CON	In environments set to integration with Microsoft, if set to YES the system sends a new request on the same TCP connection (instead of opening a new one).
SIP_ENABLE_FECC	By default, FECC support for SIP endpoints is enabled at the MCU level. You can disable it by manually adding this flag and setting it to NO.
SIP_FAST_UPDATE_INTERVAL_ENV	Default setting is **0** to prevent the RMX from automatically sending an Intra request to all SIP endpoints. Enter **n** (where n is any number of seconds other than 0) to let the RMX automatically send an Intra request to all SIP endpoints every n seconds. It is recommended to set the flag to 0 and modify the frequency in which the request is sent at the endpoint level (as defined in the next flag).
SIP_FAST_UPDATE_INTERVAL_EP	Default setting is 6 to let the RMX automatically send an Intra request to Microsoft OC endpoints only, every 6 seconds. Enter any other number of seconds to change the frequency in which the RMX send the Intra request to Microsoft OC endpoints only. Enter 0 to disable this behavior at the endpoint level (not recommended).

Table 22-2 *Manually Added System Flags – MCMS_PARAMETERS (Continued)*

Flag	Description
SIP_FREE_VIDEO_RESOURCES	For use in Avaya and Microsoft Environments. When set to **NO** (required for Avaya and Microsoft environments), video resources that were allocated to participants remain allocated to the participants as long as they are connected to the conference even if the call was changed to audio only. The system allocates the resources according to the participant's endpoint capabilities, with a minimum of 1 CIF video resource. Enter YES to enable the system to free the video resources for allocation to other conference participants. The call becomes an audio only call and video resources are not guaranteed to participants if they want to add video again. Default value in Microsoft environment: NO.
SIP_TCP_PORT_ADDR_STRATEGY	Setting the flag to 1 prevents the use of two sockets for one SIP call - one for inbound traffic, one for outbound traffic. This is done by inserting port "5060/5061" into the Route[0] header. **Possible values:** • 0 - Inbound traffic on port 5060/5061 outbound traffic on port 60000 • 1 - Both inbound and outbound traffic on port 5060/5061 **Default**: 1
SITE_NAME_TRANSPARENCY (MPM+ Only)	In **MPM+ Mode** this flag is used to enable or disable transparency (50%) of the *Site Name* in the video layout. Set the value of this flag to NO to disable *Site Name Transparency.* Default: YES. In **MPMx Mode** this function is controlled using the *Profile - Site Names* dialog box.
SITE_NAMES_ALWAYS_ON (MPM+ Only)	In **MPM + Mode** this flag is used to enable or disable the permanent display of *Site Name* in the video layout. Set the value of this flag to YES to enable the permanent display of *Site Names.* Default: NO. In **MPMx Mode** this function is controlled using the *Profile - Site Names* dialog box.
SOCKET_ACTIVITY_TIMEOUT	For use in Microsoft environments. When the MS_KEEP_ALIVE *System Flag* is set to YES, the value of this flag is used as the *MS Keep-Alive Timer* value.
SUPPORT_HIGH _PROFILE	Enables or disables the support of *High Profile* video protocol in CP conferences. This flag is specific to CP conferences and has no effect on VSW conferences. Range: YES / NO Default: YES

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
SUPPORT_HIGH_PROFILE_WITH_ISDN	Enables or disables the support of *High Profile* video protocol for ISDN participants in CP conferences. This flag is specific to CP conferences and has no effect on VSW conferences. Range: YES / NO Default: NO
TC_BURST_SIZE	This flag regulates the Traffic Control buffer or maxburst size as a percentage of the participant line rate. Range: 1-30.
TC_LATENCY_SIZE	This flag limits the latency (in milliseconds) or the number of bytes that can be present in a queue. Range: 1-1000 (in milliseconds).
TCP_RETRANSMISSION_TIMEOUT	The number of seconds the server will wait for a *TCP* client to answer a call before closing the connection. Default = 5 (seconds)
V35_ULTRA_SECURED_SUPPORT	This flag must be set to YES when deploying a *Serial Gateway S4GW.*
VSW_CIF_HP_THRESHOLD_BITRATE	Controls the *Minimum Threshold Line Rate* (kbps) for *CIF* resolution for *High Profile-enabled VSW conferences*. Default: 64
VSW_HD1080p_HP_THRESHOLD_BITRATE	Controls the *Minimum Threshold Line Rate* (kbps) for *HD1080p* resolution for *High Profile-enabled VSW conferences*. Default: 1024
VSW_HD720p30_HP_THRESHOLD_BITRATE	Controls the *Minimum Threshold Line Rate* (kbps) for *HD720p30* resolution for *High Profile-enabled VSW conferences*. Default: 512
VSW_HD720p50-60_HP_THRESHOLD_BITRATE	Controls the *Minimum Threshold Line Rate* (kbps) for *HD720p50* and *HD720p50* resolutions for *High Profile-enabled VSW conferences*. Default: 832
VSW_RATE_TOLERANCE_PERECENT	Determines the percentage of bandwidth that can be deducted from the required bandwidth to allow participants to connect to the conference. For example, a value of 20 will allow a participant to connect to the conference if the allocated line rate is up to 20% lower than the conference line rate (or between 80% to 100% of the required bandwidth). Range: 0 - 75 Default: 0
VSW_SD_HP_THRESHOLD_BITRATE	Controls the *Minimum Threshold Line Rate* (kbps) for *SD* resolution for *High Profile-enabled VSW conferences*. Default: 128

Table 22-2 Manually Added System Flags – MCMS_PARAMETERS (Continued)

Flag	Description
WRONG_NUMBER_DIAL_RETRIES	The number of re-dial attempts for a wrong destination number or a wrong destination number time-out. Range: 0 - 5 Default: 3 A flag value of 0 means that no redials are attempted.

4 Click **OK** to close the *New Flag* dialog box.
The new flag is added to the flags list.

5 Click **OK** to close the *System Flags* dialog box.

For flag changes (including deletion) to take effect, reset the MCU. For more information see "*Resetting the RMX"* on page **21-69**.

Manually Adding Flags to the CS_MODULE_PARAMETERS Tab

Using the procedure to manually add flags to the System Configuration, the following flags can be manually added to the **CS_MODULE_PARAMETERS** tab:

Table 22-3 Manually Added Flags - CS_MODULE_PARAMETERS Tab

Flag	Description
CS_ENABLE_EPC	Add this flag with the value **YES** (default value is NO) to enable endpoints that support People+Content and require a different signaling (for example, FX endpoints) to receive Content.
H245_TUNNELING	For use in the Avaya Environment. In the Avaya Environment, set the flag to YES to ensure that H.245 is tunneled through H.225. Both H.245 and H.225 will use the same signaling port. Default: NO.
H323_RAS_IPV6	If the RMX is configured for *IPv4 & IPv6* addressing, *RAS* (*Registration, Admission,* and *Status*) messages are sent in both *IPv4* and *IPv6* format. If the gatekeeper cannot operate in *IPv6* addressing mode, registration fails and endpoints cannot connect using the RMX prefix. In such cases this *System Flag* should be set to **NO**. Default: **YES**
H323_TIMERS_SET_INDEX	Enables or disables H.323 index timer according to standard or proprietary H.323 protocol. Possible values: 0 (Default) - Sets the H.323 index timer to Polycom proprietary. 1 - Sets the H.323 index timer based on the H.323 Standard recommendation. **Note:** For homologation and certification testing, this flag must be set to 1.

***Table 22-3** Manually Added Flags - CS_MODULE_PARAMETERS Tab*

Flag	Description
MS_UPDATE_CONTACT_REMOVE	When the flag value is set to: • **YES** - The *Contact Header* is removed from the *UPDATE* message that is sent periodically to the endpoints. This is required when the *SIP Server Type* field of the *IP Network Service* is set as **Microsoft.** Removal of the *Contact Header* from the UPDATE message is required specifically by *OCS R2*. • **NO** - The *Contact Header* is included in the *UPDATE* message. This is the system behavior when the *SIP Server Type* is set as **Generic**. This is required when the RMX is configured to accept calls from both *Microsoft LYNC* and *Cisco CUCM* as *CUCM* requires the *Contact Header*.
QOS_IP_SIGNALING	Used to select the priority of IP packets when *DiffServ is* the is the selected method for packet priority encoding. Range: 0x## Default: 0x00
SIP_DUAL_DIRECTION_TCP_CON	For use in Microsoft environments. When set to YES, sends a new request on the same TCP connection instead of opening a new connection. Range: YES/NO Default: NO
SIP_ST_ENFORCE_VAL	For use in Microsoft environments. Session timer interval in seconds. Default = YES
SIP_TIMERS_SET_INDEX	SIP Timer type timeout settings according to standard or proprietary protocol. Possible values are: 0 - Default 1 - SIP Standard recommendation. **Note:** For homologation and certification testing, this flag must be set to 1.
SIP_TO_TAG_CONFLICT	For use in Microsoft environments. In case of forking, a tag conflict will be resolved when Status 200 OK is received from an answering UA. Default: YES

Deleting a Flag

To delete a flag:

1 In the *System Flags* dialog box, select the flag to delete and click the **Delete Flag** button.

2 In the confirmation message box, click **Yes** to confirm.

3 Click **OK to** close the *System Flags* dialog box.

Auto Layout Configuration

The *Auto Layout* option lets the RMX automatically select the conference video layout based on the number of participants currently connected to the conference. You can modify the default selection of the conference video layout to customize it to your conferencing preferences.

Customizing the Default Auto Layout

The default *Auto Layout* is controlled by 13 flags:

PREDEFINED_AUTO_LAYOUT_0, ... , PREDEFINED_AUTO_LAYOUT_12

Each of the 11 *Auto Layout* flags can be left at its default value, or set to any of the *Possible Values* listed in Table 22-4.

The flag that controls the *Auto Layout* you wish to modify must be added to the *System Configuration* file. For more information see "*Modifying System Flags"* on page **22-1**.

Table 22-4 *Flags: PREDEFINED_AUTO_LAYOUT_0,...,10*

Flag Name: PREDEFINED_AUTO_LAYOUT_n (n = Number of Participants)		
n	**Default Value**	**Possible Values**
0	CP_LAYOUT_1X1	CP_LAYOUT_1X1
1	CP_LAYOUT_1X1	CP_LAYOUT_1X2
2	CP_LAYOUT_1X1	CP_LAYOUT_1X2HOR
3	CP_LAYOUT_1x2VER	CP_LAYOUT_1X2VER
4	CP_LAYOUT_2X2	CP_LAYOUT_2X1
5	CP_LAYOUT_2X2	CP_LAYOUT_1P2HOR
6	CP_LAYOUT_1P5	CP_LAYOUT_1P2HOR_UP
7	CP_LAYOUT_1P5	CP_LAYOUT_1P2VER
8	CP_LAYOUT_1P7	CP_LAYOUT_2X2
9	CP_LAYOUT_1P7	CP_LAYOUT_1P3HOR_UP
10	CP_LAYOUT_1P7	CP_LAYOUT_1P3VER
11	CP_LAYOUT_2P8	CP_LAYOUT_1P4HOR
12	CP_LAYOUT_1P12	CP_LAYOUT_1P4HOR_UP

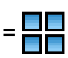
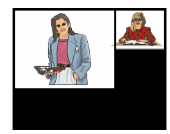
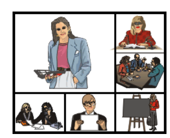
Table 22-4 Flags: PREDEFINED_AUTO_LAYOUT_0,...,10 (Continued)

Flag Name: PREDEFINED_AUTO_LAYOUT_n (n = Number of Participants)		
n	**Default Value**	**Possible Values**
		CP_LAYOUT_1P4VER
		CP_LAYOUT_1P5
		CP_LAYOUT_1P7
		CP_LAYOUT_1P8UP
		CP_LAYOUT_1P8CENT
		CP_LAYOUT_1P8HOR_UP
		CP_LAYOUT_3X3
		CP_LAYOUT_2P8
		CP_LAYOUT_1P12
		CP_LAYOUT_4X4

Example:

Table 22-5 illustrates the effect of modifying the **`PREDEFINED_AUTO_LAYOUT_5`** flag in conferences with fewer or more participants than the number of windows selected in the default layout.

***Table 22-5** Example: Modifying PREDEFINED_AUTO_LAYOUT_5 Flag*

Flag	Set to Possible Value	Number of Participants	Participant's View
PREDEFINED _AUTO_LAYOUT_5 *Default =* 	CP_LAYOUT _1x2VER 	3	 Voice activated switching displays the current speaker in the left window of the video layout and only the two last speakers are displayed.
		7	
	CP_LAYOUT _1P5 	3	 Voice activated switching displays the current speaker in the large (top left) window of the video layout.
		7	 Voice activated switching displays the current speaker in the top left window of the video layout.

LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values

Table 22-6 lists the value for each video layout that can be defined for the LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag. It allows the selection of video layout that will be displayed on the screen of the legacy endpoint when switching to Content mode.

***Table 22-6** LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values*

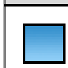
Layout	Flag Value
	CP_LAYOUT_1X1

Table 22-6 LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values (Continued)

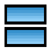
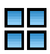
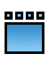
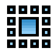
Layout	Flag Value
	CP_LAYOUT_1X2
	CP_LAYOUT_1X2HOR
	CP_LAYOUT_1X2VER
	CP_LAYOUT_2X1
	CP_LAYOUT_1P2HOR
	CP_LAYOUT_1P2HOR_UP
	CP_LAYOUT_1P2VER
	CP_LAYOUT_2X2
	CP_LAYOUT_1P3HOR_UP
	CP_LAYOUT_1P3VER
	CP_LAYOUT_1P4HOR_UP
	CP_LAYOUT_1P4HOR
	CP_LAYOUT_1P4VER
	CP_LAYOUT_1P5
	CP_LAYOUT_1P7
	CP_LAYOUT_1P8UP
	CP_LAYOUT_1P8CENT
	CP_LAYOUT_1P8HOR_UP
	CP_LAYOUT_3X3

Table 22-6 LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values (Continued)

Layout	Flag Value
	CP_LAYOUT_2P8
	CP_LAYOUT_1P12
	CP_LAYOUT_4X4

CS_ENABLE_EPC Flag

Endpoints that support *People+* may require a different signaling (for example, FX endpoints). For these endpoints, manually add the flag **CS_ENABLE_EPC** with the value **YES** (default value is NO) to the **CS_MODULE_PARAMETERS** tab.

Automatic Password Generation Flags

The RMX can be configured to automatically generate conference and chairperson passwords when the *Conference Password* and *Chairperson Password* fields are left blank.

Guidelines

- If the flag **HIDE_CONFERENCE_PASSWORD** is set to **YES**, the automatic generation of passwords (both conference and chairperson passwords) is disabled, regardless of the settings of the flags NUMERIC_CONF_PASS_DEFAULT_LEN and NUMERIC_CHAIR_PASS_ DEFAULT _LEN.
- The automatic generation of conference passwords is enabled/disabled by the flag NUMERIC_CONF_PASS_DEFAULT_LEN.
- The automatic generation of chairperson passwords is enabled/disabled by the flag NUMERIC_CHAIR_PASS_ DEFAULT _LEN.
- The automatically generated passwords will be numeric and random.
- The passwords are automatically assigned to ongoing conferences, Meeting Rooms and Reservations at the end of the creation process (once they are added to the RMX).
- Automatically assigned passwords can be manually changed through the *Conference/ Meeting Room/Reservation Properties* dialog boxes.
- Deleting an automatically created password will not cause the system to generate a new password and the new password must be added manually or the field can be left blank.
- If a password was assigned to the conference via Microsoft Outlook using the PCO add-in, the system does not change these passwords and additional passwords will not be generated (for example, if only the conference password was assigned a chairperson password will not be assigned).
- If the flag values (i.e. the password lengths) are changed, passwords that were already assigned to conferences, Meeting Rooms and Reservations will not change and they can

be activated using the existing passwords. Only new conferencing entities will be affected by the change.

Do not enable this option in an environment that includes a *Polycom DMA* system.

Enabling the Automatic Generation of Passwords

To enable the automatic generation of passwords, the following flags have to be defined:

Table 22-7 Automatic Password Generation Flags

Flag	Description
HIDE_CONFERENCE_PASSWORD	**NO (default)** - Conference and chairperson passwords are displayed when viewing the Conference/Meeting Room/ Reservation properties. It also enables the automatic generation of passwords in general. **Yes** - Conference and Chairperson Passwords are hidden (they are replaced by asterisks). It also disables the automatic generation of passwords.
NUMERIC_CONF_PASS_MIN_LEN	Enter the minimum number of characters required for conference passwords. Possible values: **0 – 16**. **0 (default in non-secured mode)** means no minimum length. However this setting cannot be applied when the RMX is in *Ultra Secure Mode*. **9 (default in Ultra Secure Mode)** Conference password must be at least 9 characters in length.
NUMERIC_CHAIR_PASS_MIN_LEN	Enter the minimum number of characters required for chairperson passwords. Possible values: **0 – 16**. **0 (default in non-secured mode)** means no minimum length. However this setting cannot be applied when the RMX is in *Ultra Secure Mode*. **9 (default in Ultra Secure Mode)**, Chairperson password must be at least 9 characters in length.
NUMERIC_CONF_PASS_MAX_LEN	Enter the maximum number of characters permitted for conference passwords. Possible values: **0 – 16** (non-secured mode) or **9 – 16** (Ultra Secure Mode). **16 (default)** - Conference password maximum length is 16 characters.
NUMERIC_CHAIR_PASS_MAX_LEN	Enter the maximum number of characters permitted for chairperson passwords. Possible values: **0 – 16** (non-secured mode) or **9 – 16** (Ultra Secure Mode). **16 (default)** - chairperson password maximum length is 16 characters.

Table 22-7 *Automatic Password Generation Flags (Continued)*

Flag	Description
NUMERIC_CONF_PASS_DEFAULT_LEN	This flag enables or disables the automatic generation of conference passwords. The length of the automatically generated passwords is determined by the flag value. Possible values: • **0 – 16, 6 default** (non-secured mode) • **0 and 9 – 16, 9 default** (Ultra Secure Mode). Enter **0** to disable the automatic generation of passwords. Any value other than 0 enables the automatic generation of conference passwords provided the flag *HIDE_CONFERENCE_PASSWORD is set to NO.* If the default is used, in non-secured mode the system will automatically generate conference passwords that contain 6 characters.
NUMERIC_CHAIR_PASS_ DEFAULT_LEN	This flag enables or disables the automatic generation of chairperson passwords. The length of the automatically generated passwords is determined by the flag value. Possible values: • **0 – 16, 6 default** (non-secured mode) • **0 and 9 – 16, 9 default** (Ultra Secure Mode). Enter **0** to disable the automatic generation of passwords. Any value other than 0 enables the automatic generation of chairperson passwords provided the flag *HIDE_CONFERENCE_PASSWORD is set to NO.* If the default is used, in non-secured mode the system will automatically generate chairperson passwords that contain 6 characters.

If the default password length defined by the NUMERIC_CONF_PASS_DEFAULT_LEN or NUMERIC_CHAIR_PASS_ DEFAULT LEN does not fall within the range defined by the minimum and maximum length an appropriate fault is added to the Faults list.

Flags Specific to Maximum Security Environments - Ultra Secure Mode

The RMX can operate in one of two modes: *Standard Security Mode* or *Ultra Secure Mode*.

In *Ultra Secure Mode* the enhanced security features of the version are rigorously enforced.

The *Ultra Secure Mode* is enabled or disabled depending on the value of the **ULTRA_SECURE_MODE** *System Flag*.

Ultra Secure Mode, is enabled by manually adding the **ULTRA_SECURE_MODE** flag to the *System Configuration* and setting its value to **YES**.

Ultra Secure Mode Flag

WARNING: Once **Ultra Secure Mode** is enabled it can only be undone by performing a **Restore to Factory Defaults**. Also, to implement a Maximum Security environment, other Polycom products on the network must be similarly configured.
For more information see "*Restoring Defaults"* on page **J-1**.

When the ULTRA_SECURE_MODE flag is set to YES, Version 7.8 does not include support for:

- Connection to Alternate Management Network via LAN3 port
- SUPPORT user
- Auditor user
- Chairperson user
- Connections to External Databases
- IP Sec security protocols
- ISDN Cascade
- Serial connection
- Modem connection
- MPM cards
- SIP
- SIP security (Digest)
- SIP TLS
- SNMP
- SSH server.
- USB key configuration
- Web link (Hyperlink in Participant Properties dialog box)
- QoS with IPv6
- Recording link

Guidelines

- *Ultra Secure Mode* is disabled by default and can be enabled by changing the value of the **ULTRA_SECURE_MODE** *System Flag* to **YES** during *First Entry Configuration* or at any time using the **Setup > System Configuration** menu.
- After modifying the value of the **ULTRA_SECURE_MODE** *System Flag* to **YES**, all RMX users are forced to change their *Login* passwords.
- When upgrading from a version containing a **JITC_MODE** *System Flag*, the system will automatically create an **ULTRA_SECURE_MODE** *System Flag* and set it to the value of the **JITC_MODE** flag before the upgrade.

  The system will then delete the **JITC_MODE** *System Flag*.
- When downgrading to a version that utilizes the **JITC_MODE** *System Flag*, the administrator will need to set the **JITC_MODE** flag to the value of the **ULTRA_SECURE_MODE** flag's value before the upgrade.

- The **ULTRA_SECURE_MODE** *System Flag* affects the ranges and defaults of the *System Flags* that control:
  - — Network Security
  - — User Management
  - — Strong Passwords
  - — Login and Session Management
  - — Cyclic File Systems

Table 22-8 lists the effect that setting the **ULTRA_SECURE_MODE** *System Flag* to **YES** has on all the other *Ultra Secure Mode Specific System Flags*.

For flag descriptions see "*ULTRA_SECURE_MODE System Flag Descriptions"* on page **22-51**.

***Table 22-8** ULTRA_SECURE_MODE Flag Value – Effect on System Flags*

Flag	ULTRA_SECURE_MODE =			
	YES		NO	
	Range	Default	Range	Default
Network Security				
SEPARATE_MANAGEMENT_NETWORK	YES/ NO	YES	NO	NO
Login and Session Management				
APACHE_KEEP_ALIVE_TIMEOUT	1-999	15	1-999	120
LAST_LOGIN_ATTEMPTS	YES/ NO	YES	YES/ NO	NO
MAX_KEEP_ALIVE_REQUESTS	0 - >	0		
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM	4-80	80	4-80	80
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER	4-80	20	4-80	10
SESSION_TIMOUT_IN_MINUTES	1-999	10	0-999	0
USER_LOCKOUT	YES/ NO	YES	YES/ NO	NO
USER_LOCKOUT_DURATION_IN_MINUTES	0-480	0	0-480	0
USER_LOCKOUT_WINDOW_IN_MINUTES	0-45000	60	0-45000	60

Table 22-8 *ULTRA_SECURE_MODE Flag Value – Effect on System Flags (Continued)*

Flag	ULTRA_SECURE_MODE =			
	YES		NO	
	Range	Default	Range	Default
User Management				
DISABLE_INACTIVE_USER	1-90	30	0-90	0
Strong Passwords				
FORCE_STRONG_PASSWORD_POLICY	YES	YES	YES/NO	NO
HIDE_CONFERENCE_PASSWORD	YES/NO	NO	YES/NO	NO
HIDE_CONFERENCE_PASSWORD	YES/NO	NO	YES/NO	NO
MAX_CONF_PASSWORD_REPEATED_CHAR	1 - 4	2		
MAX_PASSWORD_REPEATED_CHAR	1 - 4	2		
MIN_PASSWORD_LENGTH	15-20	15	0-20	0
MIN_PWD_CHANGE_FREQUENCY_IN_DAYS	1-7	1	0-7	0
NUMERIC_CHAIR_PASS_MIN_LEN	9-16	9	0-16	0
NUMERIC_CONF_PASS_MIN_LEN	9-16	9	0-16	0
PASS_EXP_DAYS_MACHINE		365		
PASSWORD_EXPIRATION_DAYS	7-90	60	0-90	0
PASSWORD_EXPIRATION_WARNING_DAYS	7-14	7	0-14	0
PASSWORD_HISTORY_SIZE	10-16	10	0-16	0

Table 22-8 *ULTRA_SECURE_MODE Flag Value – Effect on System Flags (Continued)*

Flag	ULTRA_SECURE_MODE =			
	YES		NO	
	Range	Default	Range	Default
Cyclic File Systems				
ENABLE_CYCLIC_FILE_SYSTEM_ALARMS	YES/NO	YES	YES/NO	NO

ULTRA_SECURE_MODE System Flag Descriptions

Table 22-9 ULTRA_SECURE_MODE *System Flag Descriptions*

Flag	Description
Network Security	
SEPARATE_MNGT_NETWORK	When this System Flag is set to YES, all signaling between IP endpoints and the RMX is via the LAN 2 port, while all RMX management sessions are hosted via the LAN 3 port.
Login and Session Management	
APACHE_KEEP_ALIVE_TIMEOUT	The time allowed for the connection between a client and the Apache Server to be idle before the connection is terminated.
LAST_LOGIN_ATTEMPTS	The system can display a record of the last Login of the user. It is displayed in the Main Screen of the RMX Web Client or RMX Manager. To enable it, set this System Flag to YES.
MAX_KEEP_ALIVE_REQUESTS	The number of 15-second APACHE_KEEP_ALIVE_TIMEOUT request intervals for the Apache server. A value of 2880 keeps the server alive for 12 hours while a value of 5760 keeps the server alive for 24 hours. Default: 0 (This value should **never** be used)
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM	The maximum number of management sessions per system is determined by the value of this System Flag. Any attempt to exceed the maximum number of management sessions per system is recorded as an Audit Event.
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER	The maximum number of management sessions per user is determined by the value of this System Flag. Any attempt to exceed the maximum number of management sessions per user is recorded as an Audit Event.
SESSION_TIMEOUT_IN_MINUTES	If there is no input from the user or if the connection is idle for longer than the number of minutes specified by the setting of this System Flag, the connection to the RMX is terminated. A flag value of 0 means Session Timeout is disabled, This feature cannot be disabled when the RMX is in Ultra Secure mode.

Table 22-9 ULTRA_SECURE_MODE *System Flag Descriptions*

Flag	Description
USER_LOCKOUT	User Lockout can be enabled to lock a user out of the system after three consecutive Login failures with same User Name. The user is disabled and only the administrator can enable the user within the system. User Lockout is enabled when the flag is set to YES
USER_LOCKOUT_DURATION_IN_MINUTES	The duration of the Lockout of the user is determined by the value of this System Flag. A flag value of 0 means permanent User Lockout until the administrator re-enables the user within the system.
USER_LOCKOUT_WINDOW_IN_MINUTES	The time period during which the three consecutive Login failures occur is determined by the value of this System Flag. A flag value of 0 means that three consecutive Login failures in any time period will result in User Lockout.
User Management	
DISABLE_INACTIVE_USER	The value of this System Flag determines the number of consecutive days a user can be inactive before being disabled.
Strong Passwords	
FORCE_STRONG_PASSWORD_POLICY	This System Flag, enables or disables all password related flags. It cannot be set to NO when the RMX is in Ultra Secure Mode
HIDE_CONFERENCE_PASSWORD	Conference and Chairperson Passwords that are displayed in the *RMX Web Client* or *RMX Manager* can be hidden when viewing the properties of the conference. When the value of this System Flag is set to YES, these passwords are replaced by asterisks in the *RMX Web Client*, *RMX Manager,* Audit Event and Log files.
MAX_CONF_PASSWORD_REPEATED_CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters that are to be allowed in a conference password. Range: 1 - 4 Default: 2
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER _SYSTEM	Any attempt to exceed the maximum number of management sessions per system as specified by the value of this System Flag is recorded as an Audit Event.
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER _USER	Any attempt to exceed the maximum number of management session per user as specified by the value of this System Flag is recorded as an Audit Event.
MAX_PASSWORD_REPEATED_CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a password. Range: 1 - 4 Default: 2
MIN_PASSWORD_LENGTH	The length of passwords is determined by the value of this System Flag. It cannot be set to NO when the RMX is in Ultra Secure Mode.

Table 22-9 ULTRA_SECURE_MODE *System Flag Descriptions*

Flag	Description
MIN_PWD_CHANGE_FREQUENCY_IN_DAYS	The frequency with which a user can change a password is determined by the value of this System Flag. The value of the flag is the number of days that users must retain a password. It cannot be set to NO when the RMX is in Ultra Secure Mode.
NUMERIC_CHAIR_PASS_MIN_LEN	The length of the Chairperson password is determined by the value of this System Flag. It cannot be set to NO when the RMX is in Ultra Secure Mode.
NUMERIC_CONF_PASS_MIN_LEN	The length of the Conference password is determined by the value of this System Flag. It cannot be set to NO when the RMX is in Ultra Secure Mode.
PASS_EXP_DAYS_MACHINE	Enables the administrator to change the password expiration period of *application-user*'s independently of regular users. Default: 365 (days)
PASSWORD_EXPIRATION_WARNING_DAYS	The display of a warning to the user of the number of days until password expiration is determined by the value of this System Flag. The earliest warning can be displayed 14 days before passwords are due to expire and the latest warning can be displayed 7 days before passwords are due to expire. It cannot be set to NO when the RMX is in Ultra Secure Mode.
PASSWORD_HISTORY_SIZE	The number of passwords that are recorded is determined by the value of this System Flag. It cannot be set to NO when the RMX is in Ultra Secure Mode.
Cyclic File Systems	
ENABLE_CYCLIC_FILE_SYSTEM_ALARMS	Setting this System Flag to YES prevents automatic deletion of Cyclic Files such as Logger, CDR and Audit Event files.
RMX Serial Gateway S4GW	
V35_ULTRA_SECURED_SUPPORT	Must be added in *system.cfg* and set to YES when configuring an *RMX Serial Gateway S4GW.* Range: YES / NO Default: NO

23

RMX Hardware Monitoring

The status and properties of the RMX hardware components can be viewed and monitored in the *Hardware Monitor* list pane.

Viewing the Status of the Hardware Components

The *Hardware Monitor's* status column displays the present status of the hardware components. In addition to the status, temperature and voltage indications are provided for each component.

The MCU's Shelf Management Server is what users are connecting to when accessing the *Hardware Monitor* pane. This pane can be accessed in either two ways: through the *RMX Web Client* or the Shelf Management Server. Connection via the Shelf Management Server enables users to access the *Hardware Monitor* even when the connection through the *RMX Web Client* is unavailable. The ability to connect directly via the Shelf Management Server enables users to: enter the *Hardware Monitor* and view the problematic hardware components, reset and restart the MCU and run diagnostics. Running diagnostics and restarting the MCU can only be done via direct connection to the Shelf Management Server.

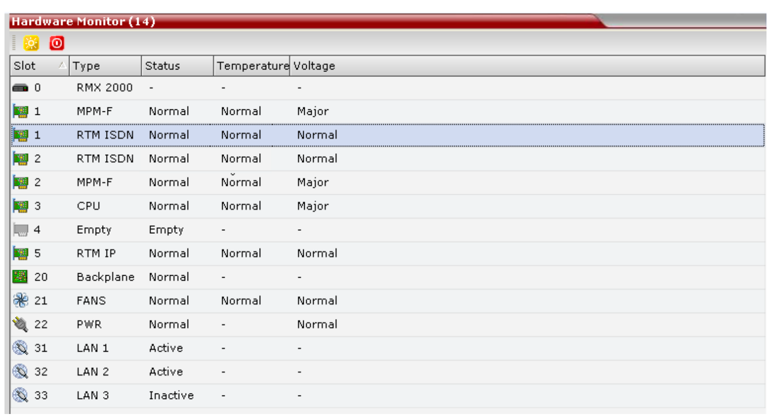
For more information, see "*Diagnostic Mode (RMX 1500/2000/4000)"* on page **23-21**

When accessing the Shelf Management server, the content displayed will be available in English only.

To view the status of the Hardware Components on the RMX 1500/2000/4000:

>> In the *RMX Management* pane, click the **Hardware Monitor** button.

The *Hardware Monitor* pane is displayed.



Hardware Monitor (14)

Slot	Type	Status	Temperature	Voltage
0	RMX 2000	-	-	-
1	MPM-F	Normal	Normal	Major
1	RTM ISDN	Normal	Normal	Normal
2	RTM ISDN	Normal	Normal	Normal
2	MPM-F	Normal	Normal	Major
3	CPU	Normal	Normal	Major
4	Empty	Empty	-	-
5	RTM IP	Normal	Normal	Normal
20	Backplane	Normal	-	-
21	FANS	Normal	Normal	Normal
22	PWR	Normal	-	Normal
31	LAN 1	Active	-	-
32	LAN 2	Active	-	-
33	LAN 3	Inactive	-	-

In the Hardware Monitor, Slots 1 & 2 may sometimes appear as duplicates in the Slot list.

The *Hardware Monitor* pane displays the following RMX hardware component's status columns:

Table 23-1 *HW Monitor Pane Status Columns*

Field	Description
Slot	Displays an icon according to the HW component type and the slot number. The icon displays the hardware status as follows: • An exclamation point (**!**) indicates errors in the HW component. • Card icon with the reset button () indicates that the HW component is currently resetting. • Card icon with diagnostic tools () indicates that the HW component is in diagnostic mode.
Type	The type of hardware component card.
Status	The current status of the HW component; *Normal, Major, Critical, Resetting, Diagnostics, or Empty.*
Temperature	Monitors the temperature of the hardware components; Normal, Major and Critical. **Note:** Critical condition invokes a system shut down.
Voltage	The voltage threshold of the hardware component; either *Normal* or *Major*.

HW Monitor Pane Tool bar

The following buttons appear in the tool bar of the Hardware Monitor:

Table 23-2 *HW Monitor Pane Tool Bar Buttons*

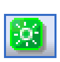
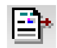
Button	Name	Description
	*System Reset*	Resets and restarts the system. Resetting saves settings and information that you changed in the system, i.e. IP Services, etc...
	*System Shut Down*	Shuts down the system into a standby mode. When the user in the *RMX Manager/Client* presses the *System Shut Down* (red) button in the H*ardware Monitor* tool bar, the system should enter a standby mode and the LED turns ON. Only the media and control unit cards are in a standby mode. Shelf Manager remains active. Turn the system OFF/ON to exit the standby mode.
	*System Start Up*	Starts up the system. **Note:** This button is only displayed when connecting directly to the Shelf Management server.
	*Shelf Manager*	In the HW Monitor this opens the Shelf Management login window. In the Shelf Management HW Monitor this sets the MFA, CPU and Switch (Cards: MPM/MPM+/MPMx, CNTL and RTM IP) into diagnostic mode. For more information, see "*Diagnostic Mode (RMX 1500/2000/4000)"* on page **23-21**.

Table 23-2 *HW Monitor Pane Tool Bar Buttons (Continued)*

Button	Name	Description
	*Logger Mode*	Diagnostics Tests selection and Tests monitoring. **Note:** This button is only displayed when connecting directly to the Shelf Management server and logged in as a special support user.

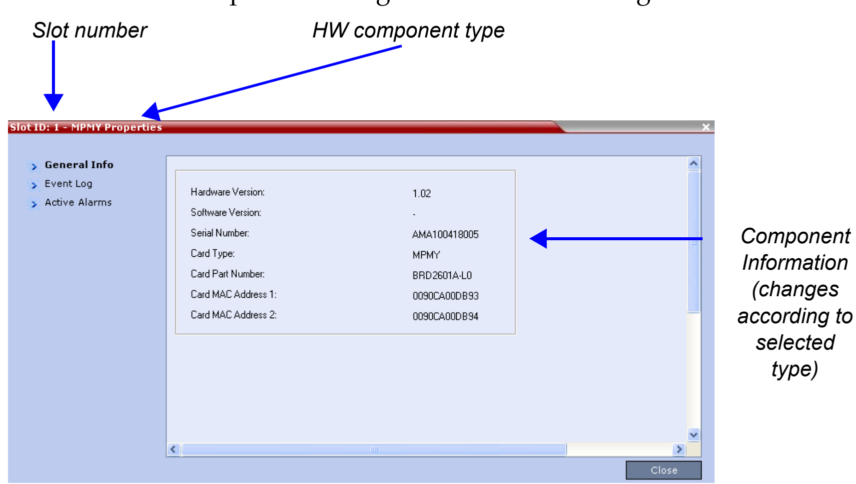
Viewing the Properties of RealPresence Collaboration Server (RMX) 1500 Hardware Components

The properties displayed for the hardware components will vary according to the type of component viewed. These component properties can be grouped as follows:

- MCU Properties (RealPresence Collaboration Server (RMX) 1500)
- Card Properties (MPMx, CPU, RTM IP, RTM ISDN)
- Supporting Hardware Components Properties (Backplane, FANS, LAN)

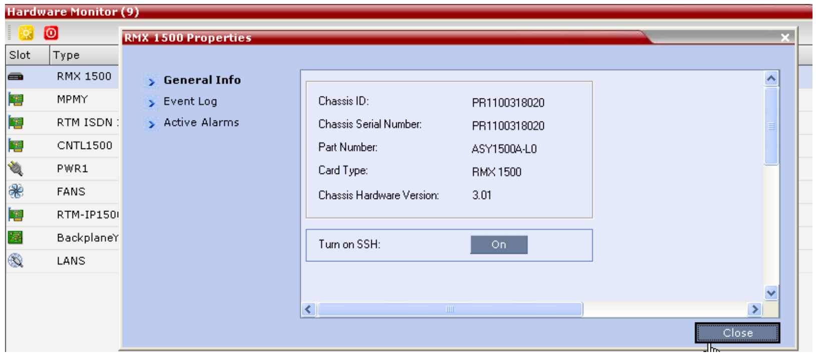
> No properties are provided for Power Supply (PWR). For more information, see the *RealPresence Collaboration Server (RMX) 1500 Hardware Guide*, "*RMX 1500 Power Supply"* on page **1-20**.

The Hardware Properties dialog box has the following structure:



To view the MCU Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **Properties** for *RMX 1500, slot 0*.

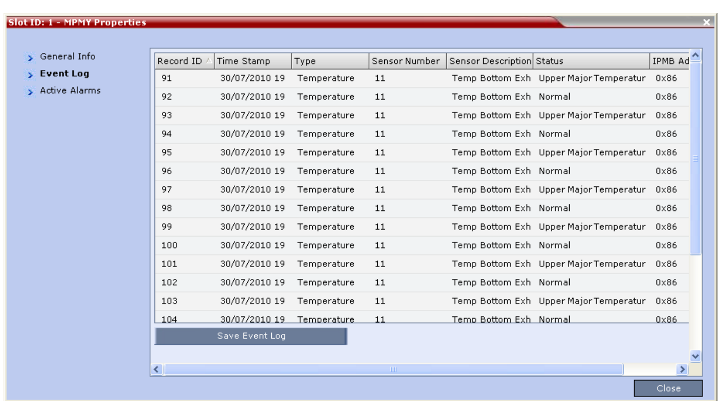


The following information is displayed:

***Table 23-3** MCU Properties - General Info*

Field	Description
Chassis File ID	The ID assigned to the MCU's chassis file.
Chassis Serial Number	The serial number assigned to the MCU's chassis.
Part Number	The chassis part number. The Part Number contains the letter A/B/C/D that represents the chassis type.
Card Type	The name of the hardware product or component, i.e. RMX 1500, Backplane.
Chassis HW Version	Indicates the MCU's current chassis hardware version.
Turn SSH	Enables/disables the SSH monitor. This is a secured terminal enabling access to the operating system in order to define Linux commands.

2 Click the *Event Log* tab to view a log of events that were recorded by the system for the RMX.

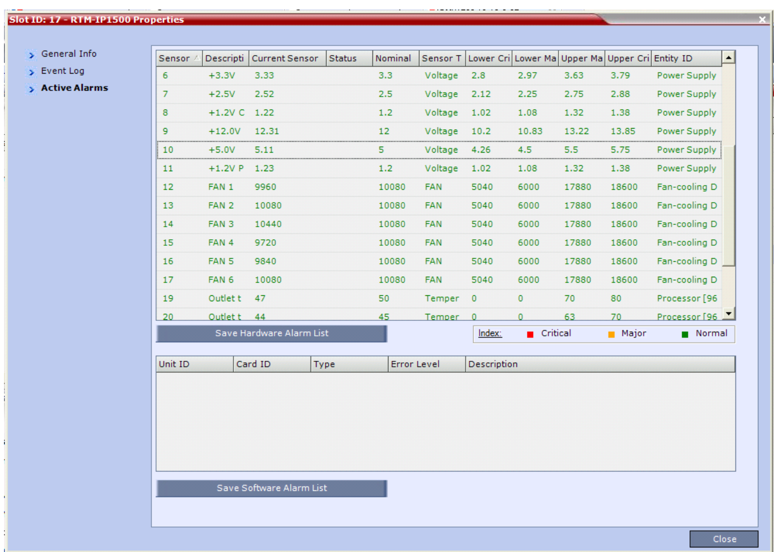


The logged events can be saved to a *.xls file by clicking the **Save Event Log** button. It is not possible to save individual or multiple selected events; the entire log file must be saved.

Table 23-4 *MCU Properties - Event Log*

Column	Description
Record ID	The recorded ID number of the logged event.
Time Stamp	Lists the date and time that the event occurred.
Type	Displays the type of event recorded in the log.
Sensor Number	The number of the LED sensor on the RMX unit.
Sensor Description	Describes which sensor the event is being logged.
Status	The sensor's active status.
Ipmb Address(hex)	Contains all the internal IPMI network addresses on the IPMB bus, i.e. 0x20 (Switch), 0x86 (MFA), etc...

3 Click the *Active Alarms* tab to view alarms related to the RMX, i.e. temperatures and main power sensors.



The *Active Alarms* dialog box displays fields that relate to faults and errors detected on the RMX by sensors. The *Active Alarms* dialog box is divided into two sections: *HW Alarm List* and *SW Alarm List*.

Each section's alarm list can be saved as a *.xls file by clicking the **Save HW Alarm List** and **Save SW Alarm List** buttons respectively. Each alarm list color codes the severity of the alarm; Critical (RED), Major (ORANGE) and Normal (GREEN).

If you connected to the Hardware Monitoring via the Shelf Management server, the *SW Alarm List* section will not be displayed.

To view the Card Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **properties** for the desired hardware component.

The following information is displayed:

Table 23-5 Card Properties - General Info

Field	Description
Hardware Version	The hardware component's version number.
Software Version	The version number of the software installed on card.
Serial Number	The hardware component's serial number.
Card Type	Displays the type of card that occupies the slot.
Card Part Number	The part number of the HW component's board.
Card Mac Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Card MAC Address 2	(If applicable) second MAC address.
Mezzanine A	
Hardware Version	The Mezzanine A hardware component's version number.
Serial Number	The Mezzanine A hardware component's serial number.
Card Part Number	The part number of the Mezzanine A hardware component's board.
Mezzanine B	
Hardware Version	The Mezzanine B hardware component's version number.
Serial Number	The Mezzanine B hardware component's serial number.
Card Part Number	The part number of the Mezzanine B hardware component's board.

2 Click the **Event Log** tab to view a log of events recorded by the system on the HW component.

For more information, see "*MCU Properties - Event Log"* on page **23-11**.

3 Click the **Active Alarms** tab to view alarms related to the hardware component, i.e. temperatures and main power sensors.

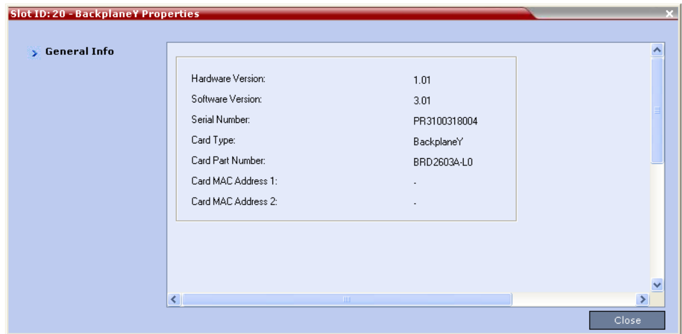
For more information, see "*Active Alarms"* on page **23-12**.

4 Click **Close** to return to the *HW Monitor* pane.

To View the Supporting Hardware Components Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select properties for the desired supporting hardware component.

The component's properties dialog box will appear with the *General Info* tab displayed.



Backplane Properties:

The RMX unit's backplane properties provides the following information:

Table 23-6 *Backplane Properties - General Info*

Field	Description
HW Version	The Backplane's current hardware version.
SW Version	The Backplane's current software version.
Serial Number	The Backplane's serial number.
Card Type	The name of the hardware component for which information is being displayed, e.g. Backplane.
Card Part Number	The Backplane's part number.
Card MAC Address 1	The Backplane's hardware address.
Card MAC Address 2	(If applicable) second Backplane MAC address.

FAN Properties:

The RMX unit's chassis contains 3 fans that regulate the unit's temperature. If the temperature increases, the fans speed will increase and vice-versa. A "Critical" condition in the fans operation will result in a system shut down.

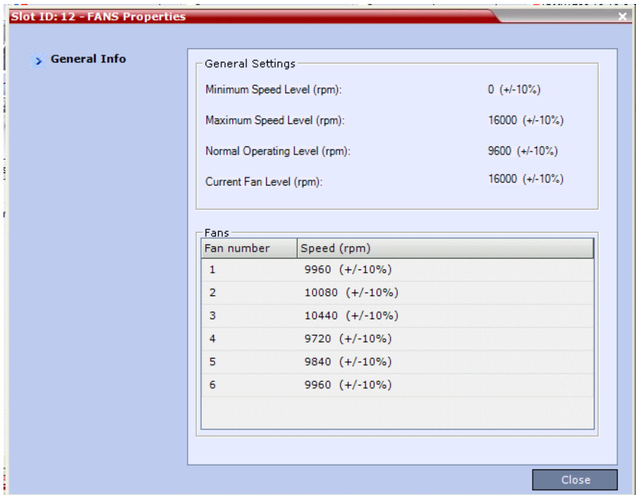


Table 23-7 FANS Properties - General Info

Field	Description
General Settings	
Min. Speed Level (rpm)	The minimum speed level of the fans.
Max. Speed Level (rpm)	The maximum speed level of the fans.
Normal Operating Level (rpm)	The normal operating level defined for the fans.
Current Fan Level (rpm)	The current operating level of the fans.
Fans	
Fan 1 Speed (rpm)	Present speed of fan 1.
Fan 2 Speed (rpm)	Present speed of fan 2.
Fan 3 Speed (rpm)	Present speed of fan 3.

LAN 1, LAN 2, LAN 3 Properties:

The RMX unit's chassis contains 3 external LAN connectors which register the following information listed below. The information will be refreshed every 8 seconds and also contains a peek detector to log the maximal values, since the last peek values reset.

2 Click **Close** to return to the *HW Monitor* pane.

Viewing the Properties of RealPresence Collaboration Server (RMX) 2000 Hardware Components

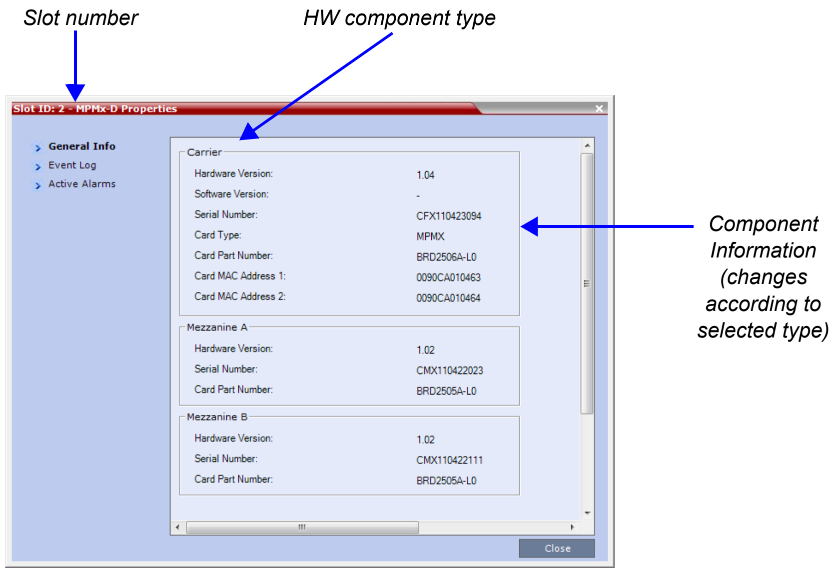
The properties displayed for the hardware components will vary according to the type of component viewed. These component properties can be grouped as follows:

- MCU Properties (RealPresence Collaboration Server (RMX) 2000)
- Card Properties (MPM/F/P, MPM+, MPMx, CPU, RTM IP, RTM ISDN, RTM LAN)
- Supporting Hardware Components Properties (Backplane, FANS, LAN)

> No properties are provided for Power Supply (PWR). For more information, see the *RealPresence Collaboration Server (RMX) 2000 Hardware Guide*, "*RMX 2000 Specifications"* on page **1-2**.

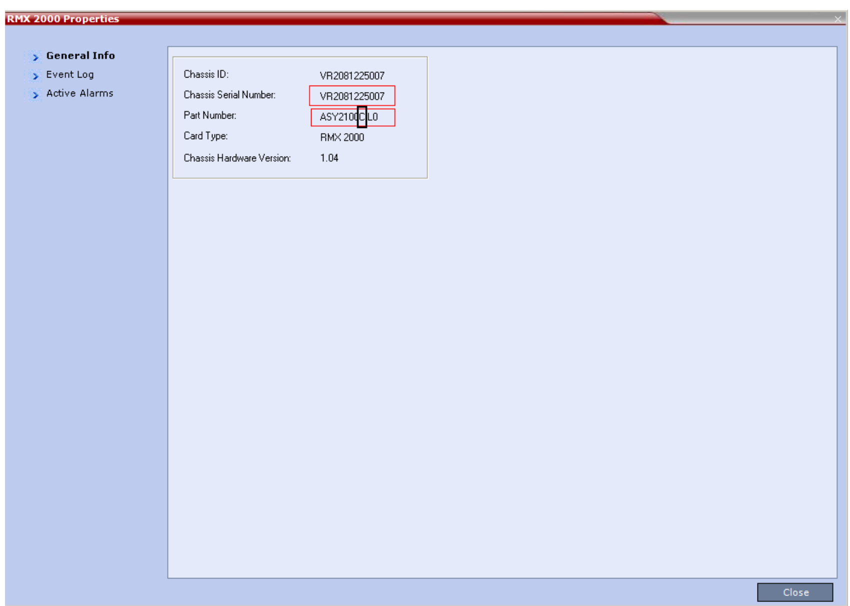
> From *Version 7.1*, *MPM* media cards are not supported.

The Hardware Properties dialog box has the following structure:



To view the MCU Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **properties** for *RMX 2000, slot 0*.



The following information is displayed:

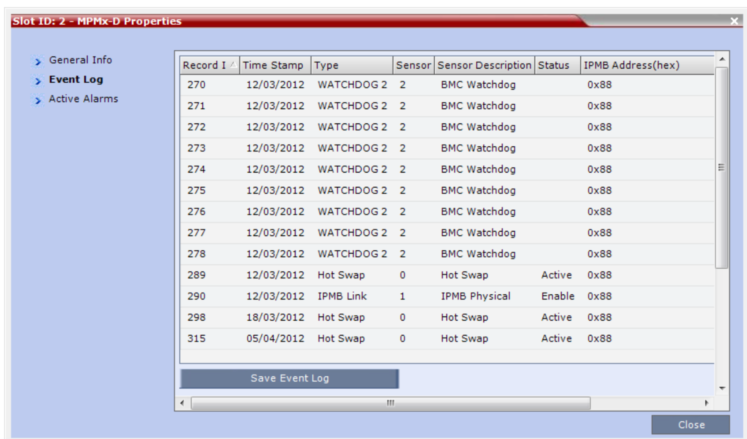
Table 23-8 MCU Properties - General Info

Field	Description
Chassis File ID	The ID assigned to the MCU’s chassis file.

***Table 23-8** MCU Properties - General Info (Continued)*

Field	Description
Chassis Serial Number	The serial number assigned to the MCU's chassis.
Part Number	The chassis part number. The Part Number contains the letter A/B/C/D that represents the chassis type.
Card Type	The name of the hardware product or component, i.e. RMX 2000, Backplane.
Chassis HW Version	Indicates the MCU's current chassis hardware version.
Turn SSH	Enables/disables the SSH monitor. This is a secured terminal enabling access to the operating system in order to define Linux commands.

2 Click the *Event Log* tab to view a log of events that were recorded by the system for the RMX.



The logged events can be saved to a *.xls file by clicking the **Save Event Log** button. It is not possible to save individual or multiple selected events; the entire log file must be saved.

***Table 23-9** MCU Properties - Event Log*

Column	Description
Record ID	The recorded ID number of the logged event.
Time Stamp	Lists the date and time that the event occurred.
Type	Displays the type of event recorded in the log.
Sensor Number	The number of the LED sensor on the RMX unit.
Sensor Description	Describes which sensor the event is being logged.
Status	The sensor's active status.

Table 23-9 MCU Properties - Event Log (Continued)

Column	Description
Ipmb Address(hex)	Contains all the internal IPMI network addresses on the IPMB bus, i.e. 0x20 (Switch), 0x86 (MFA), etc...

3 Click the *Active Alarms* tab to view alarms related to the RMX, i.e. temperatures and main power sensors.

The *Active Alarms* dialog box displays fields that relate to faults and errors detected on the RMX by sensors. The *Active Alarms* dialog box is divided into two sections: *HW Alarm List* and *SW Alarm List*.

Each section's alarm list can be saved as a *.xls file by clicking the **Save HW Alarm List** and **Save SW Alarm List** buttons respectively. Each alarm list color codes the severity of the alarm; Critical (RED), Major (ORANGE) and Normal (GREEN).

If you connected to the Hardware Monitoring via the Shelf Management server, the *SW Alarm List* section will not be displayed.

To view the Card Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **properties** for the desired hardware component.

The following information is displayed:

Table 23-10 Card Properties - General Info

Field	Description
HW Version	The hardware component's version number.
SW Version	The version number of the software installed on card.

Table 23-10 Card Properties - General Info (Continued)

Field	Description
Serial Number	The hardware component's serial number.
Card Type	Displays the type of card that occupies the slot.
Card Part Number	The part number of the HW component's board.
Card MAC Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Card MAC Address 2	(If applicable) second Mac address.

2 Click the **Event Log** tab to view a log of events that was recorded by the system on the HW component.

For more information, see "*MCU Properties - Event Log*" on page **23-11**.

3 Click the **Active Alarms** tab to view alarms related to the hardware component, i.e. temperatures and main power sensors.

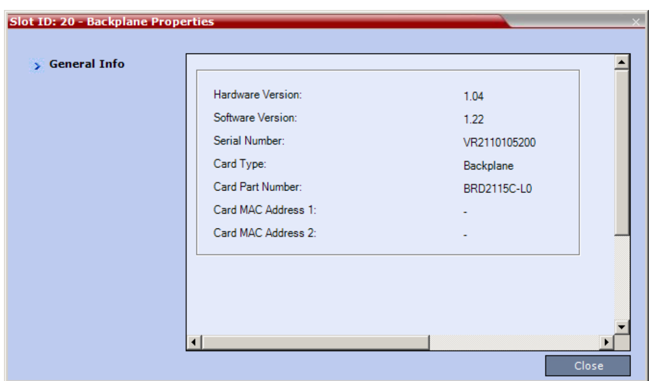
For more information, see "*Active Alarms*" on page **23-12**.

4 Click **Close** to return to the *HW Monitor* pane.

To View the Supporting Hardware Components Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select properties for the desired supporting hardware component.

The component's properties dialog box will appear with the *General Info* tab displayed.



Backplane Properties:

The RMX unit's backplane properties provides the following information:

Table 23-11 Backplane Properties- General Info

Field	Description
HW Version	The Backplane's current hardware version.
SW Version	The Backplane's current software version.
Serial Number	The Backplane's serial number.
Card Type	The name of the hardware component for which information is being displayed, e.g. Backplane.

Table 23-11 *Backplane Properties- General Info (Continued)*

Field	Description
Card Part Number	The Backplane's part number.
Card Mac Address 1	The Backplane's hardware address.
Card Mac Address 2	(If applicable) second Backplane Mac address.

FAN Properties:

The RMX unit's chassis contains 3 fans that regulate the unit's temperature. If the temperature increases, the fans speed will increase and vice-versa. A "Critical" condition in the fans operation will result in a system shut down.

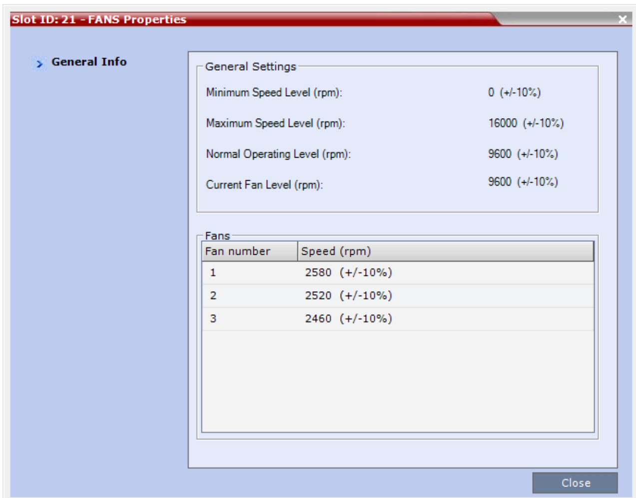
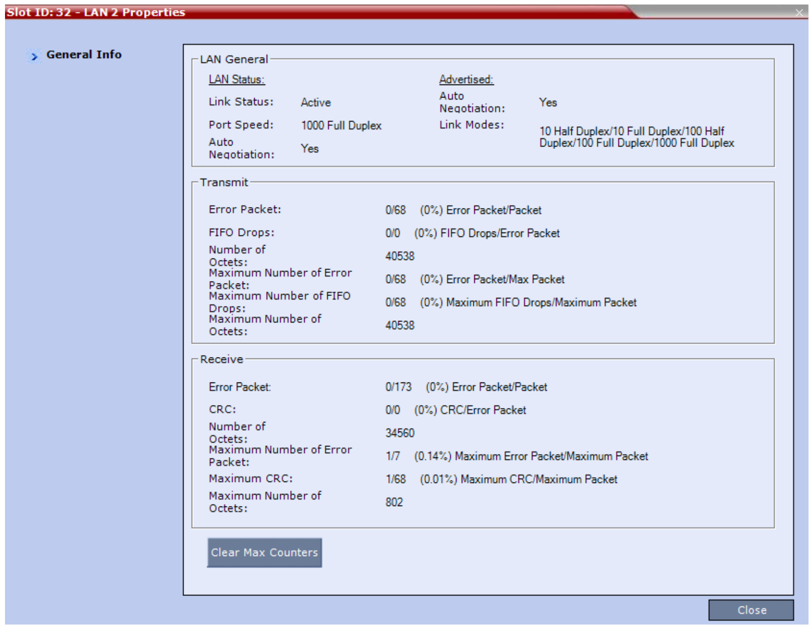


Table 23-12 *FANS Properties - General Info*

Field	Description
General Settings	
Min. Speed Level (rpm)	The minimum speed level of the fans.
Max. Speed Level (rpm)	The maximum speed level of the fans.
Normal Operating Level (rpm)	The normal operating level defined for the fans.
Current Fan Level (rpm)	The current operating level of the fans.
Fans	
Fan number (1-3)	Fan numbering.
Speed (rpm)	Present speed of a fan (1-3).

LAN 0, LAN 1, LAN 2 Properties:

The RMX unit's chassis contains 3 external LAN connectors which register the following information listed below. The information will be refreshed every 8 seconds and also contains a peek detector to log the maximal values, since the last peek values reset.



2 Click **Close** to return to the *HW Monitor* pane.

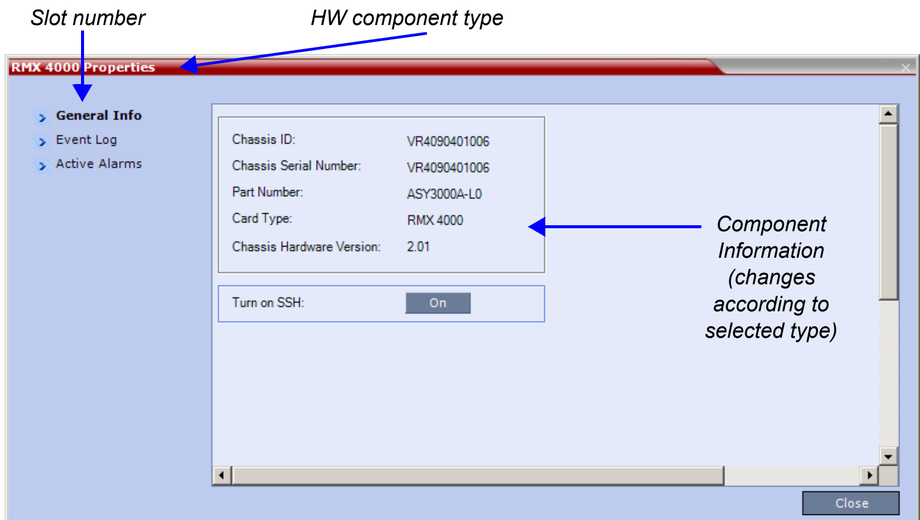
Viewing the Properties of RealPresence Collaboration Server (RMX) 4000 Hardware Components

The properties displayed for the hardware components will vary according to the type of component viewed. These component properties can be grouped as follows:

- MCU Properties (RealPresence Collaboration Server (RMX) 4000)
- Card Properties (MPM+/MPMx, CNTL 4000, RTM-IP 4000, RTM ISDN, RTM LAN)
- Supporting Hardware Components Properties (Backplane, FANS, LAN)

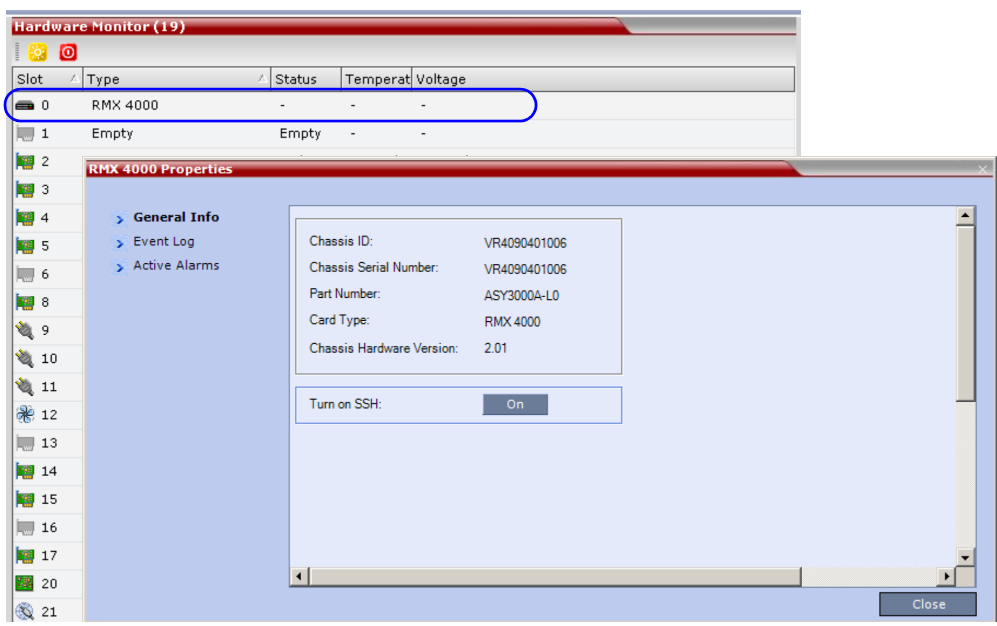
> No properties are provided for Power Supply (PWR). For more information, see the *RealPresence Collaboration Server (RMX) 4000 Hardware Guide*.

The Hardware Properties dialog box has the following structure:



To view the MCU Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **Properties** for *RMX 4000, slot 0*.



The following information is displayed:

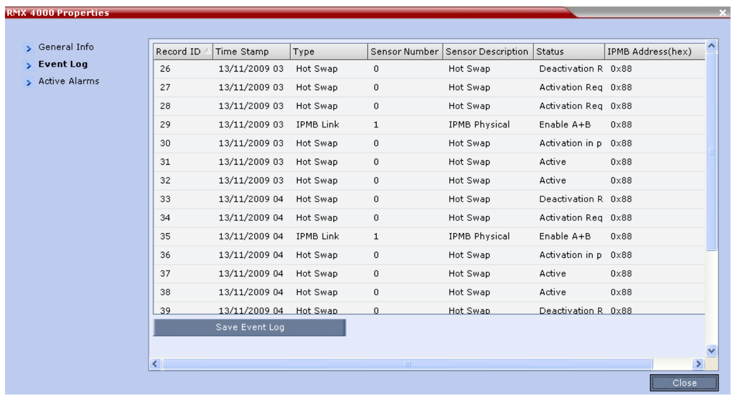
***Table 23-13** MCU Properties - General Info*

Field	Description
Chassis File ID	The ID assigned to the MCU's chassis file.
Chassis Serial Number	The serial number assigned to the MCU's chassis.

Table 23-13 MCU Properties - General Info (Continued)

Field	Description
Part Number	The chassis part number. The Part Number contains the letter A/B/C/D that represents the chassis type.
Card Type	The name of the hardware product or component, i.e. RMX 4000, Backplane.
Chassis HW Version	Indicates the MCU's current chassis hardware version.
Turn SSH	Enables/disables the SSH monitor. This is a secured terminal enabling access to the operating system in order to define Linux commands.

2 Click the *Event Log* tab to view a log of events that were recorded by the system for the RMX.

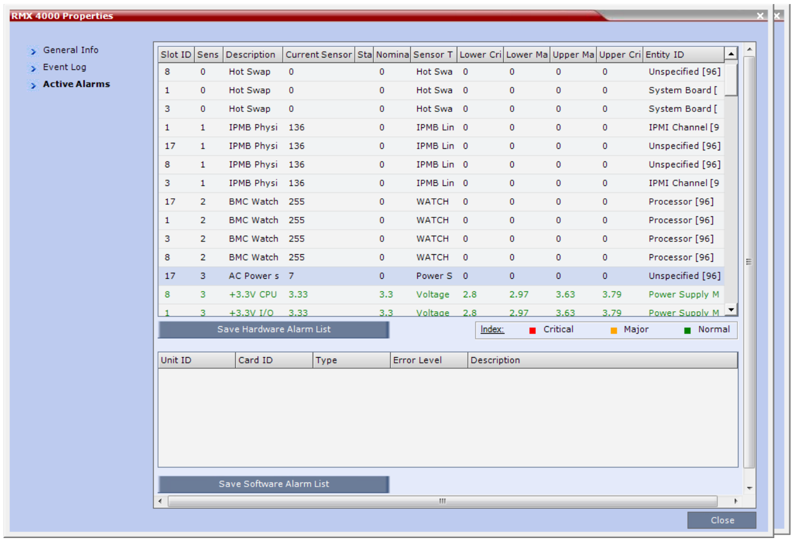


The logged events can be saved to a *.xls file by clicking the **Save Event Log** button. It is not possible to save individual or multiple selected events; the entire log file must be saved.

Table 23-14 MCU Properties - Event Log

Column	Description
Record ID	The recorded ID number of the logged event.
Time Stamp	Lists the date and time that the event occurred.
Type	Displays the type of event recorded in the log.
Sensor Number	The number of the LED sensor on the RMX unit.
Sensor Description	Describes which sensor the event is being logged.
Status	The sensor's active status.
Ipmb Address(hex)	Contains all the internal IPMI network addresses on the IPMB bus, i.e. 0x20 (Switch), 0x86 (MFA), etc...

3 Click the *Active Alarms* tab to view alarms related to the RMX, i.e. temperatures and main power sensors.



The *Active Alarms* dialog box displays fields that relate to faults and errors detected on the RMX by sensors. The *Active Alarms* dialog box is divided into two sections: *HW Alarm List* and *SW Alarm List*.

Each section's alarm list can be saved as a *.xls file by clicking the **Save HW Alarm List** and **Save SW Alarm List** buttons respectively. Each alarm list color codes the severity of the alarm; Critical (RED), Major (ORANGE) and Normal (GREEN).

If you connected to the Hardware Monitoring via the Shelf Management server, the *SW Alarm List* section will not be displayed.

To view the Card Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **Properties** for the desired hardware component.

The following information is displayed:

Table 23-15 Card Properties - General Info

Field	Description
HW Version	The hardware component's version number.
SW Version	The version number of the software installed on card.
Serial Number	The hardware component's serial number.
Card Type	Displays the type of card that occupies the slot.
Board Part Number	The part number of the HW component's board.
Board Mac Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Board Mac Address 2	(If applicable) second Mac address.

2 Click the **Event Log** tab to view a log of events that was recorded by the system on the HW component.

For more information, see "*MCU Properties - Event Log*" on page **23-11**.

3 Click the **Active Alarms** tab to view alarms related to the hardware component, i.e. temperatures and main power sensors.

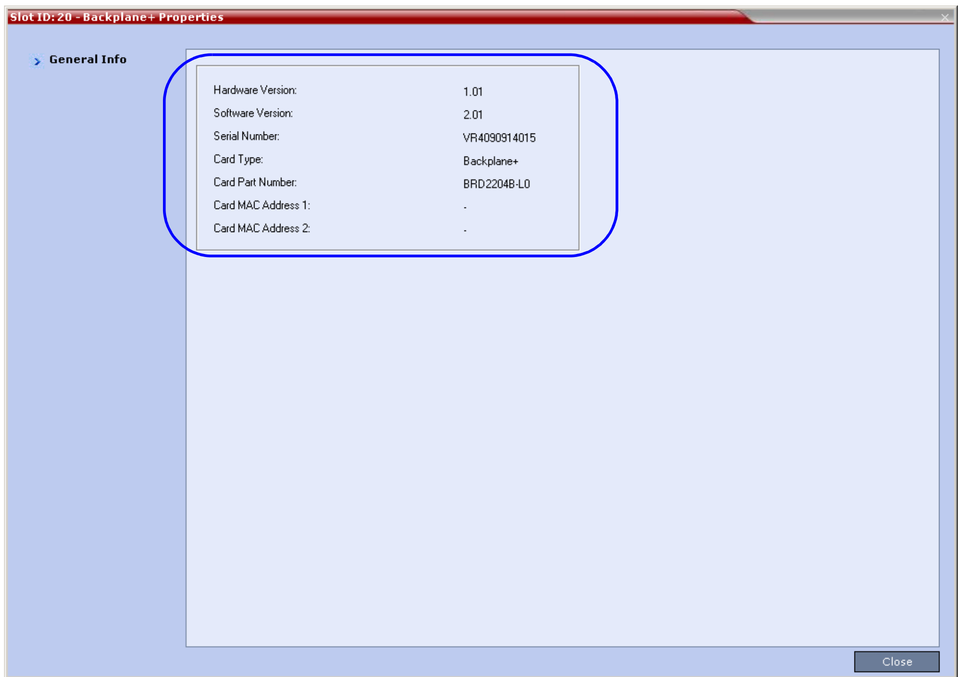
For more information, see "*Active Alarms*" on page **23-12**.

4 Click **Close** to return to the *HW Monitor* pane.

To View the Supporting Hardware Components Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select properties for the desired supporting hardware component.

The component's properties dialog box will appear with the *General Info* tab displayed.



Backplane+ Properties:

The RMX unit's backplane properties provides the following information:

Table 23-16 Backplane+ Properties- General Info

Field	Description
HW Version	The Backplane's current hardware version.
SW Version	The Backplane's current software version.
Serial Number	The Backplane's serial number.
Card Type	The name of the hardware component for which information is being displayed, e.g. Backplane.
Board Part Number	The Backplane's part number.
Board Mac Address 1	The Backplane's hardware address.

Table 23-16 Backplane+ Properties- General Info (Continued)

Field	Description
Board Mac Address 2	(If applicable) second Backplane Mac address.

FAN Properties:

The RMX unit's chassis contains 3 fans that regulate the unit's temperature. If the temperature increases, the fans speed will increase and vice-versa. A "Critical" condition in the fans operation will result in a system shut down.

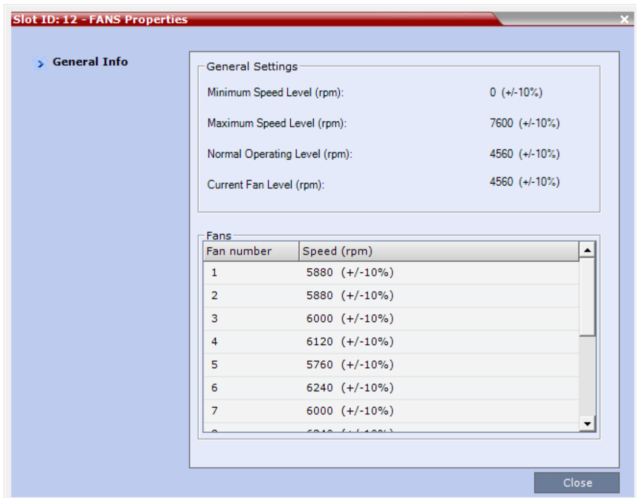
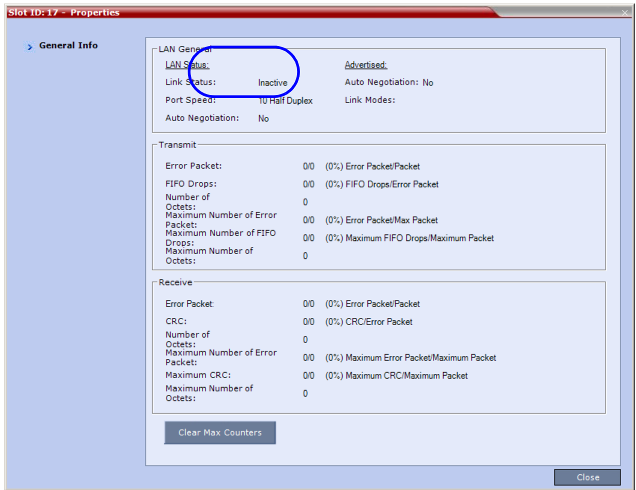


Table 23-17 FANS Properties - General Info

Field	Description
General Settings	
Min. Speed Level (rpm)	The minimum speed level of the fans.
Max. Speed Level (rpm)	The maximum speed level of the fans.
Normal Operating Level (rpm)	The normal operating level defined for the fans.
Current Fan Level (rpm)	The current operating level of the fans.
Fans	
Fan number (1-8)	Fan numbering.
Speed (rpm)	Present speed of a fan (1-8).

LAN 0, LAN 1, LAN 2 Properties:

The RMX unit's chassis contains 3 external LAN connectors which register the following information listed below. The information will be refreshed every 8 seconds and also contains a peek detector to log the maximal values, since the last peek values reset.



2 Click **Close** to return to the *HW Monitor* pane.

Diagnostic Mode (RMX 1500/2000/4000)

- You cannot run diagnostics on the MPM card.
- On all RMX systems with version 7.0.2 & 7.6.1 slight changes were made to temperature regulation and thresholds, resulting in more efficient responses by the system Fans.

Diagnostic Mode is a debugging tool for performing hardware diagnostics that detect malfunctions in the hardware component's performance. Diagnostics are performed only for the MFA, CPU and Switch (Cards: MPM+/MPMx, CPU, RTM IP and RTM ISDN). Two types of Diagnostic Modes are available:

- Basic Mode
- Advanced Mode

A user using an Administrator Login, will be able to view and access the *Basic Mode*. However, a Administrator "user" with Administrator permissions must be defined on the RMX system. For more information see "*Adding a New User"* on page **15-4**. A SUPPORT user can access both the *Basic Mode* and *Advanced Mode* Diagnostics.

When Diagnostic Mode is initialized, the MCU is reset and upon restarting, the MCU will enter Diagnostic Mode. Entering this mode causes the MCU to terminate all active conferences and prohibits conferences from being established.

Diagnostic Mode is only enabled when connecting directly to the Shelf Management server.

Connecting to the Shelf Management Server:

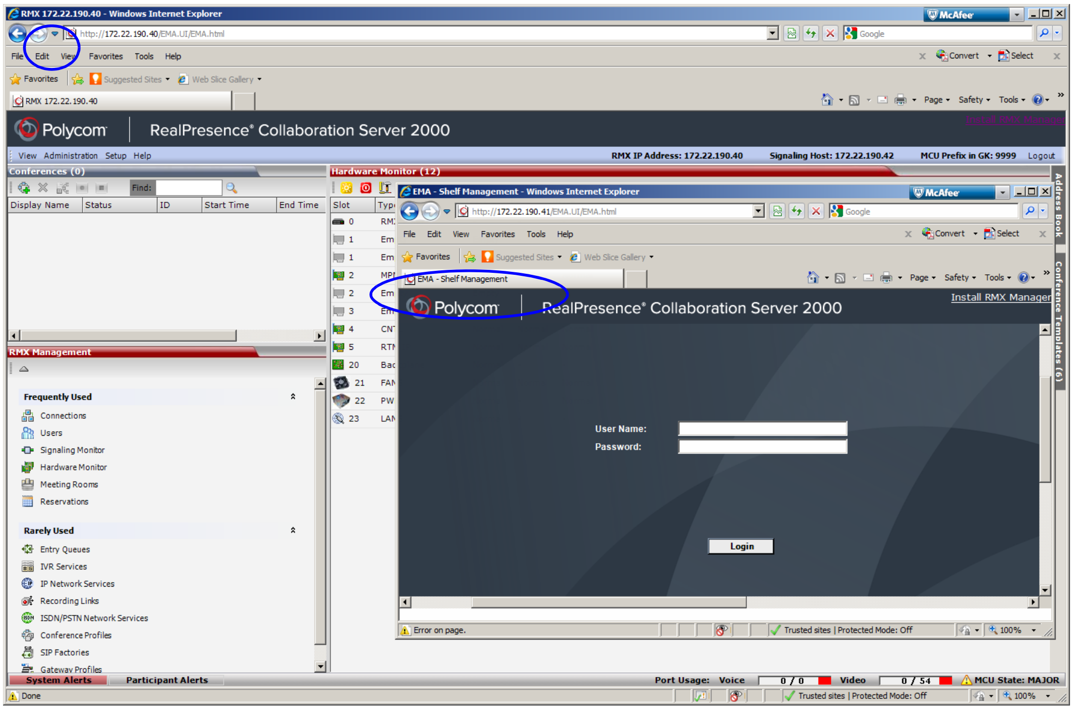
- To run Diagnostics you are required to Login with **Administrator** permissions. A user with *Administrator* permissions must be defined on the RMX.
- When accessing the Shelf Management server, the content displayed will be available in English only.

Access the RMX browser and click **Hardware Monitor**. The Hardware Monitor pane opens.

On the Hardware Monitor toolbar click the *Shelf Manager* icon.

Type in the URL address of the Shelf Management (IP address).

For example; 172.22.189.51. You must also *Login* as an “Administrator” user to run diagnostics



Login to the *Shelf Manager*.

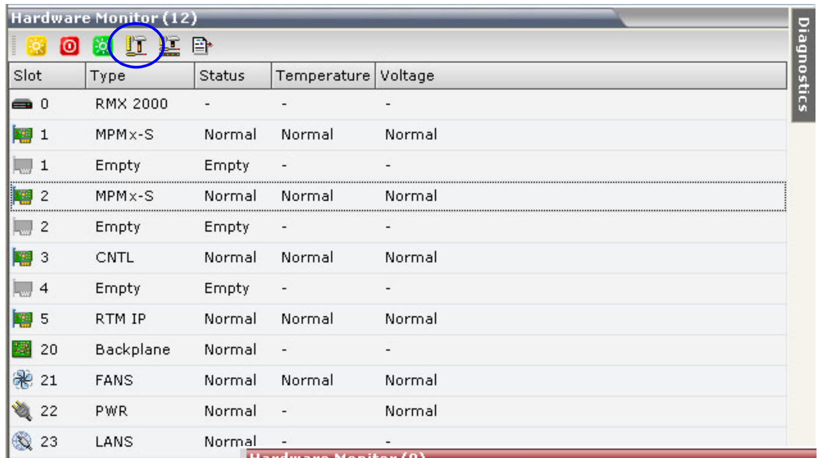
On the *Hardware Monitor* toolbar select either the **Basic Mode** or **Advanced Mode** diagnostics. Depending on your selection proceed with one of the following sections:

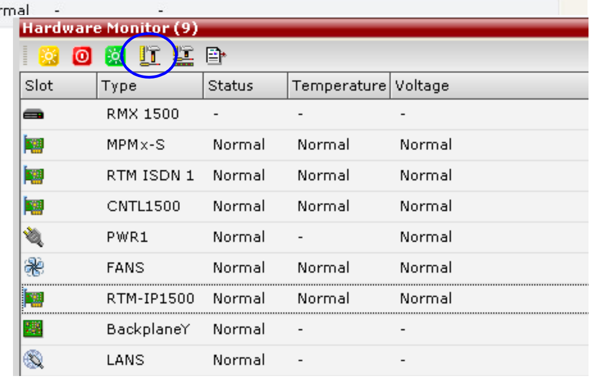
Performing Basic Mode Diagnostics

To run Basic Mode Diagnostics on a Hardware Component:

- Most of the user interfaces illustrated in this section show the RealPresence Collaboration Server (RMX) 2000 with MPMx cards. The *Basic Mode* for other RMXs with MPM+ card(s) are identical.
- On the RealPresence Collaboration Server (RMX) 1500 fewer “slots” are used and the module naming conventions used on elements are different.

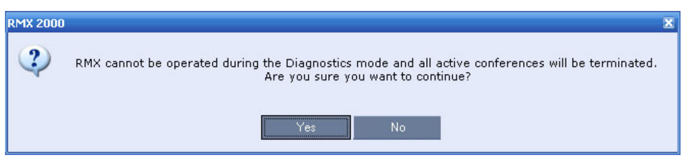
1 In the list pane tool bar, click the **Basic Mode** () button.





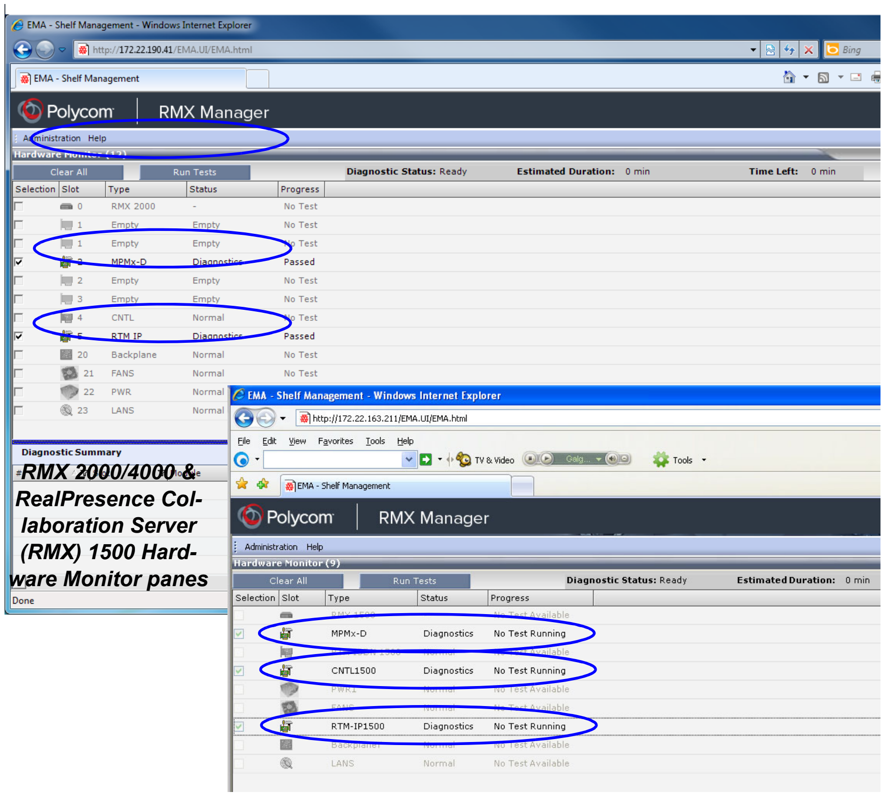
RMX 2000/4000 & RealPresence Collaboration Server (RMX) 1500 Hardware Monitor panes

2 In the *Reset Confirmation* dialog box, click **Yes**.



3 The RMX resets. Re-enter the *Shelf Manager IP address* in the browser and Login under **POLYCOM** or with an "Administrator" Login.

After login the following screen appears.



The MPM+/MPMx cards indicate “Resetting” and later switch to “Diagnostics”. The status of RTM-IP/RTM IP 1500/RTM-IP 4000 and CNTL/CNTL 1500/CNTL 4000 components change to “Diagnostics”.

4 You can select any one of the Hardware components indicating “Diagnostics/Normal” in the status column and right-click **Properties** from the menu. The card’s *General Info/ Event Log/Active Alarms* properties are displayed.

5 Run Diagnostic Tests & Tests Monitoring by clicking the **Run Tests** button. In the *Hardware Monitor* pane, the toolbar and card statuses change to *Tests in progress*.

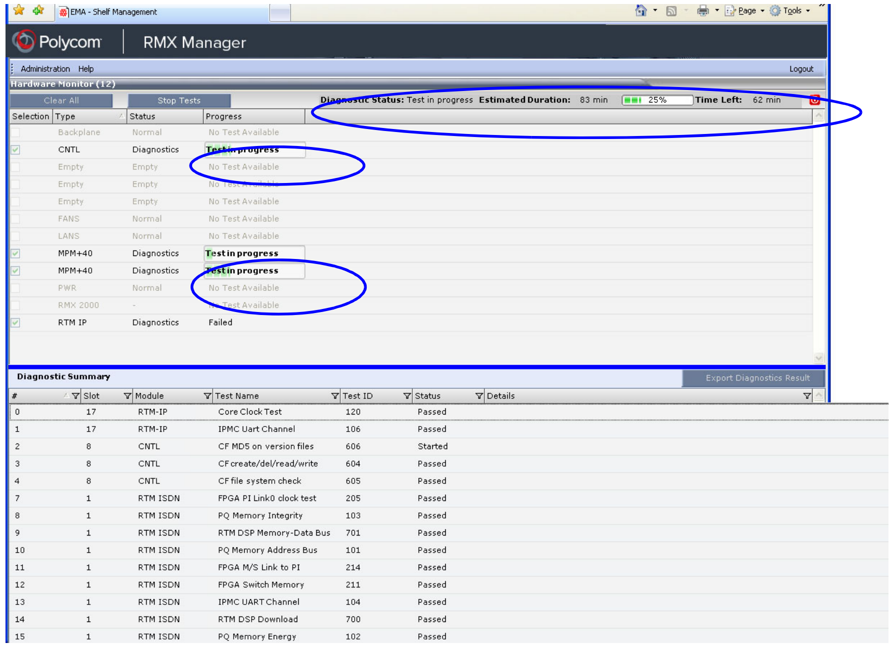
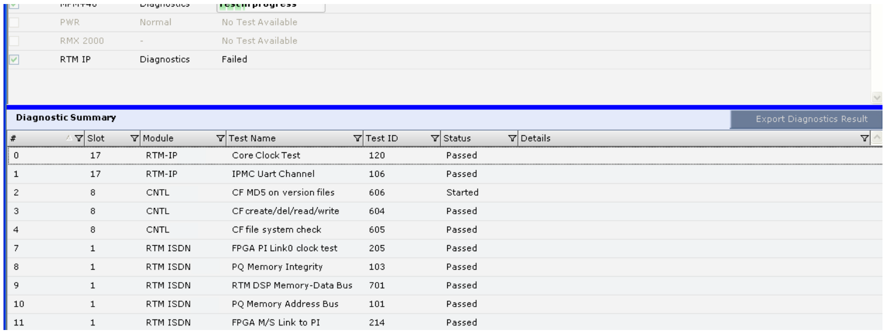


***Table 23-18** Run Tests - Parameters*

Parameter	Description
Diagnostic Status	*Basic Diagnostic Status*: • Ready - ready to run diagnostics • Test in Progress - running diagnostics • Passed/Failed - Passed/Failed the diagnostics tests
Estimated Duration	Estimated time needed to run *Basic Diagnostic* tests.
Time Left	Estimated time to complete *Basic Diagnostic* tests.

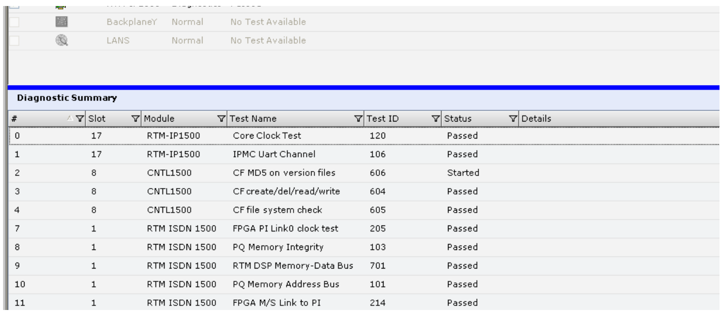
When the RMX enters "*Diagnostics Mode*", the status MPM+/MPMx, CNTL/CNTL 1500/CNTL 4000 and RTM IP/RTM IP 1500/RTM IP 4000 changes to "*Diagnostics*"

6. The *Diagnostics Summary* pane is displayed at the bottom of the *Hardware Monitoring* pane.



#	Slot	Module	Test Name	Test ID	Status	Details
0	17	RTM-IP	Core Clock Test	120	Passed	
1	17	RTM-IP	IPMC Uart Channel	106	Passed	
2	8	CNTL	CF MD5 on version files	606	Started	
3	8	CNTL	CF create/del/read/write	604	Passed	
4	8	CNTL	CF file system check	605	Passed	
7	1	RTM ISDN	FPGA PI Link0 clock test	205	Passed	
8	1	RTM ISDN	PQ Memory Integrity	103	Passed	
9	1	RTM ISDN	RTM DSP Memory-Data Bus	701	Passed	
10	1	RTM ISDN	PQ Memory Address Bus	101	Passed	
11	1	RTM ISDN	FPGA M/S Link to PI	214	Passed	

Figure 23-1 *RMX 2000/4000 Diagnostics Tests & Monitoring Tests*



#	Slot	Module	Test Name	Test ID	Status	Details
0	17	RTM-IP1500	Core Clock Test	120	Passed	
1	17	RTM-IP1500	IPMC Uart Channel	106	Passed	
2	8	CNTL1500	CF MD5 on version files	606	Started	
3	8	CNTL1500	CF create/del/read/write	604	Passed	
4	8	CNTL1500	CF file system check	605	Passed	
7	1	RTM ISDN 1500	FPGA PI Link0 clock test	205	Passed	
8	1	RTM ISDN 1500	PQ Memory Integrity	103	Passed	
9	1	RTM ISDN 1500	RTM DSP Memory-Data Bus	701	Passed	
10	1	RTM ISDN 1500	PQ Memory Address Bus	101	Passed	
11	1	RTM ISDN 1500	FPGA M/S Link to PI	214	Passed	

Figure 23-2 *RealPresence Collaboration Server (RMX) 1500 Diagnostics Tests & Monitoring Tests*

7 Select the *Run all Tests* box and then click **Run Selected Tests**.

Table 23-19 *Tests Selection - Additional Test Parameters*

Parameter	Description
Loop Test	Enter the amount of times the test is to repeat itself in succession.
Stop On Failure	Stops tests upon a failure.
Run All Test	Runs all tests listed in the *TestActive* column for the hardware component.

8 The selected tests are initialized. In the *Tests Monitoring* pane there is an indication of the *Status* of the Tests.

9 This process may take some time. Click *Stop Running Test* to end all the diagnostic tests. The MCU completes the current test running and then stops all remaining tests.

10 When the Test are completed, you have the option to download a report in Excel format for analysis by your next level of support by clicking the **Export Diagnostics Result** button.

11 The Diagnostics Mode can be exited by pressing the red *System Reset* icon.

12 The RMX then resets.

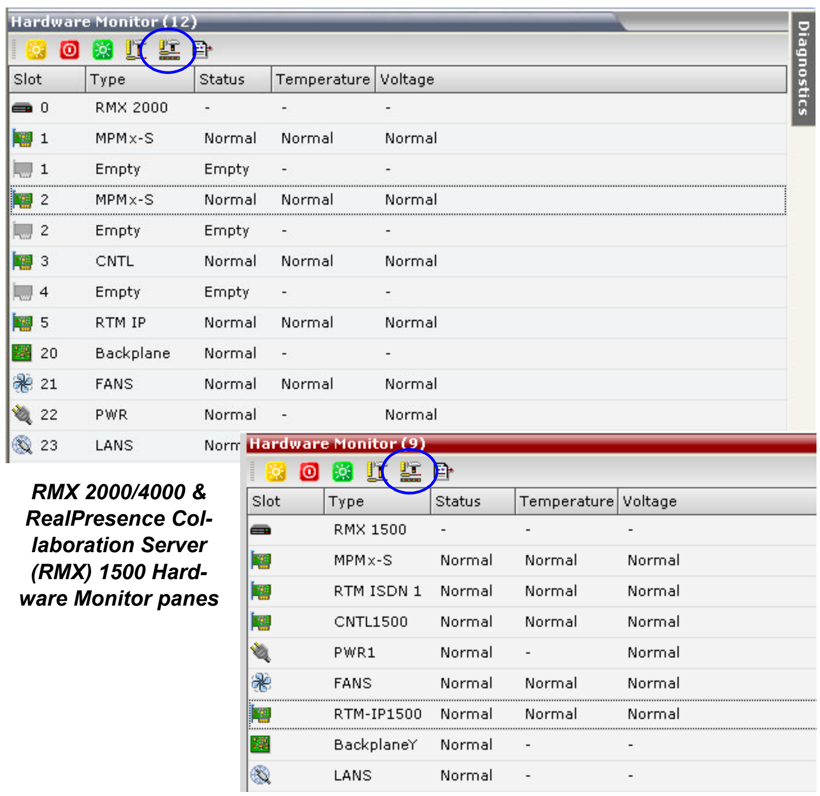
Performing Advanced Mode Diagnostics

> To run Diagnostics you are required to Login with **administrator** permissions.

To run Advanced Mode Diagnostics on a Hardware Component:

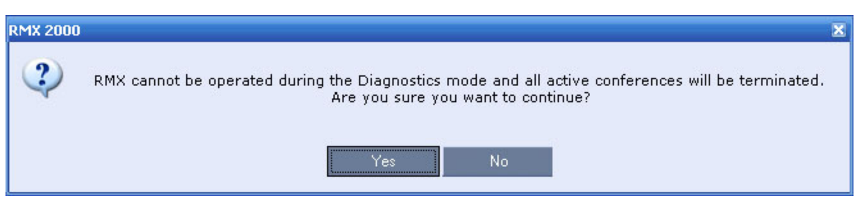
> - Most of the user interfaces illustrated in this section show the RealPresence Collaboration Server (RMX) 2000 with MPMx cards. The *Advanced Mode* for other RMXs with MPM+ card(s) are identical.
> - On the RealPresence Collaboration Server (RMX) 1500 fewer “slots” are used and the module naming conventions used on elements are different.
> - Before running Advanced Mode Diagnostic testing on the CNTL module, you must insert two formatted FAT32 USB keys in the two slots of the CNTL panel USB ports of the RMX 2000/4000. On the RealPresence Collaboration Server (RMX) 1500 insert the USB key in the front panel mouse or keyboard slot.

1 In the list pane tool bar, click the **Advanced Mode** () button.



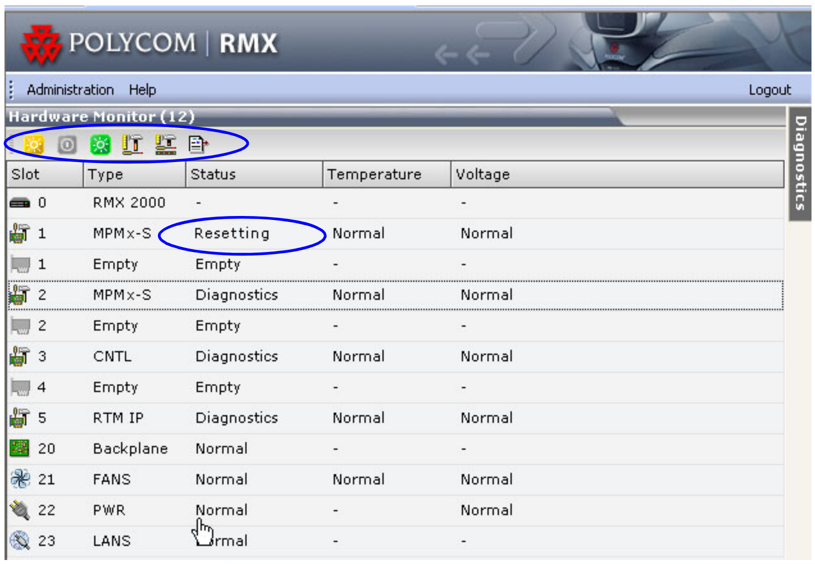
RMX 2000/4000 & RealPresence Collaboration Server (RMX) 1500 Hardware Monitor panes

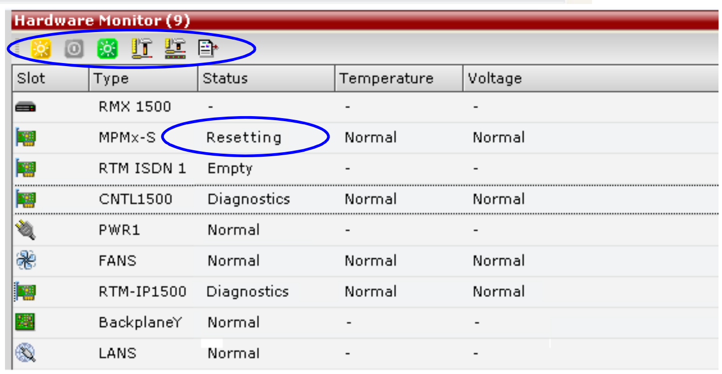
2 In the *Reset Confirmation* dialog box, click **Yes**.



3 The RMX resets. Re-enter the *Shelf Manager IP address* in the browser and Login using an "Administrator" Login.

The MPM+/MPMx cards indicate "Resetting" and later switch to "Diagnostics". The status of RTM-IP/RTM IP 1500/RTM-IP 4000 and CNTL/CNTL 1500/CNTL 4000 components change to "Diagnostics".

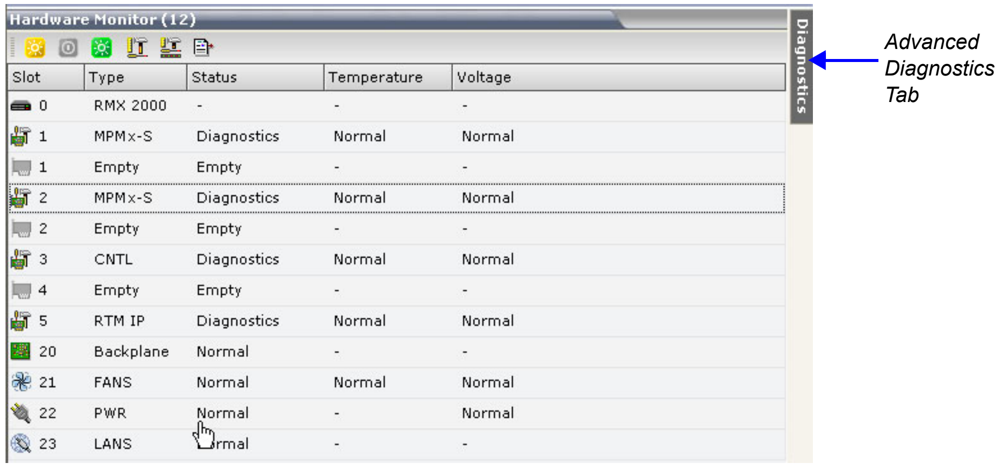




RMX 2000/4000 & RealPresence Collaboration Server (RMX) 1500Hardware Mon-

4 You can select any one of the Hardware components indicating "Diagnostics/Normal" in the status column and right-click **Properties** from the menu. The card's *General Info*/*Event Log*/*Active Alarms* properties are displayed.

You can view Diagnostic Tests & Tests Monitoring by clicking the **Advanced Diagnostics** Tab.



When you click the **Advanced Mode** the RMX enters a "Diagnostics Mode".
The *Advanced Mode* can be exited by pressing the yellow *System Reset* icon. The RMX then resets.

The *Diagnostics Tests & Monitoring Tests* panes are displayed on the right side of the window pane.

On MPM+/MPMx and all RTM IP card types, double click each card to view details of the *Test Selection* pane as shown in step 5.

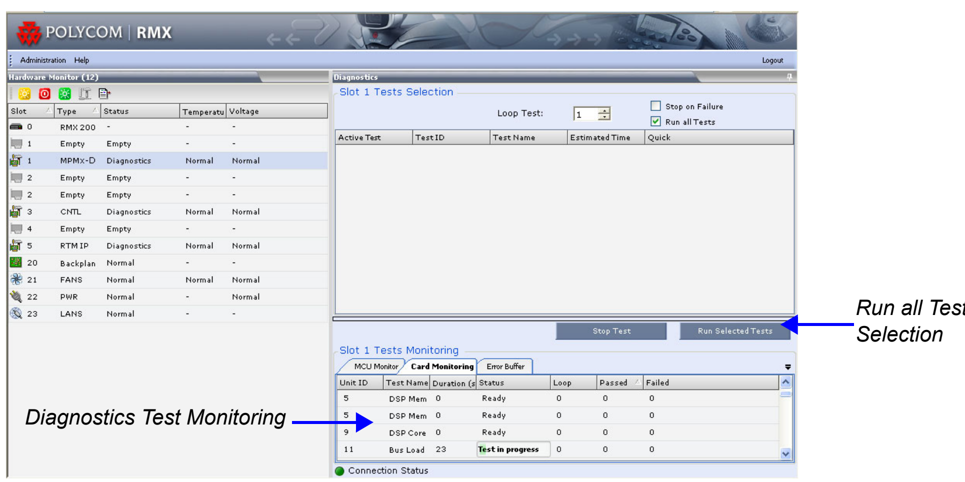


***Figure 23-3** RMX 2000/4000 Diagnostics Tests & Monitoring Tests*

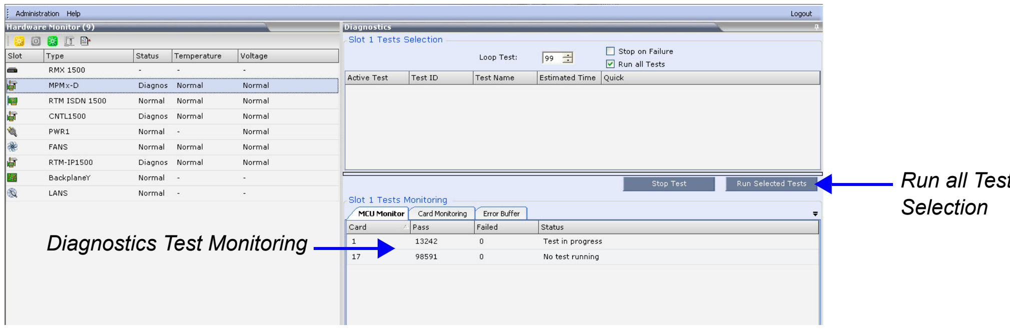


Figure 23-4 *RealPresence Collaboration Server (RMX) 1500 Diagnostics Tests & Monitoring Tests*

5 When the RMX enters "*Diagnostics Mode*", the status MPM+/MPMx, CNTL/CNTL 1500/CNTL 4000 and RTM IP/RTM IP 1500/RTM IP 4000 changes to "*Diagnostics*". You can run "*Diagnostics*" tests on a MPM+/MPMx card by **double clicking** any one of the hardware components indicating "Diagnostics" in the status column.

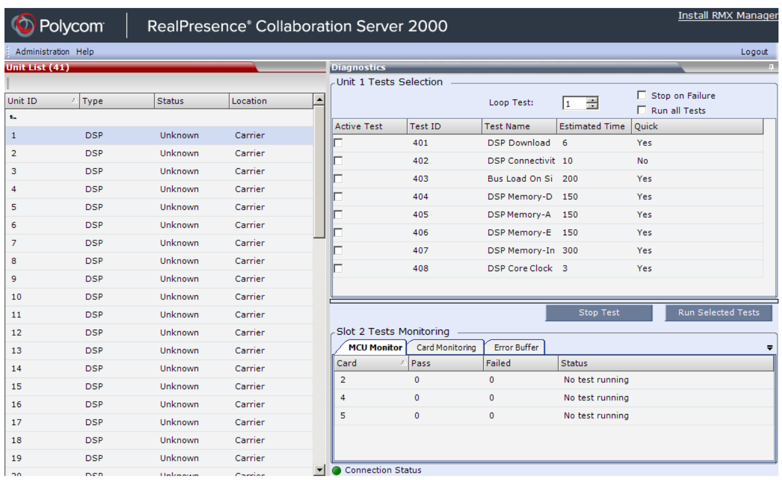


Figure 23-5 *RMX 2000/4000 MPMx D - DSP DSP Sub Test selection*

Run a "Diagnostics" test on a CTNL card by **clicking** the CTNL hardware component that indicates "Diagnostics" in the status column.

6 Select the *Run all Tests* box and then click **Run Selected Tests**.

Optional. In the *Diagnostics - Active Test* box you can select specific tests to run and then click **Run Selected Tests**.

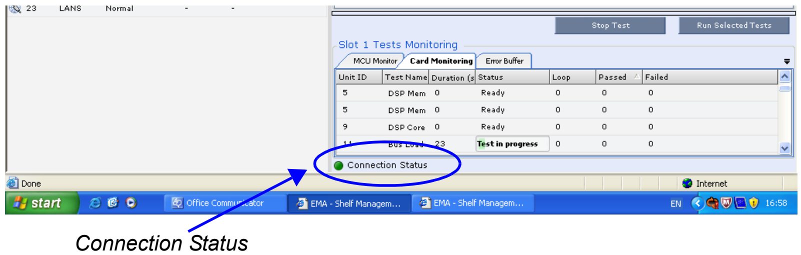
Table 23-20 *Tests Selection - Additional Test Parameters*

Parameter	Description
Loop Test	Enter the amount of times the test is to repeat itself in succession.
Stop On Failure	Stops tests upon a failure.

***Table 23-20** Tests Selection - Additional Test Parameters (Continued)*

Parameter	Description
Run All Test	Runs all tests listed in the *TestActive* column for the hardware component.

7 The selected tests are initialized. In the *Tests Monitoring* pane there is an indication of the *Connection Status* of the Tests.



8 This process may take some time. Click *Stop Running Test* to end all the diagnostic tests. The MCU completes the current test running and then stops all remaining tests.

9 The Diagnostics Mode can be exited by pressing the yellow *System Reset* icon. The RMX then resets.

Diagnostics Monitoring

A hardware component's test status can be viewed in the Diagnostics Test Monitoring section before, during and after tests have been initiated. Test results will only be displayed after tests are completed. The Diagnostic Tests Monitoring section is comprised of three tabs: *MCU Monitor, Cards Monitor* and *Error Buffer*, which are further described below.

MCU Monitor

The MCU Monitor tab lists the status of all the cards that can be tested in Diagnostic Mode. Described below are the columns:

Table 23-21 *Tests Monitoring - MCU Monitor Parameters*

Column	Description
Card	The card's slot number, i.e. 5 - slot where the RTM IP card resides.
Pass	Indicates the number of tests that the card passed successfully.
Fail	Indicates the number of tests that the card failed.
Status	The card's current test status: *No test running* or *Test in progress*.

Cards Monitor

The Cards Monitor tab displays the status of the selected tests being run on the currently viewed card, i.e. slot 5, described below.

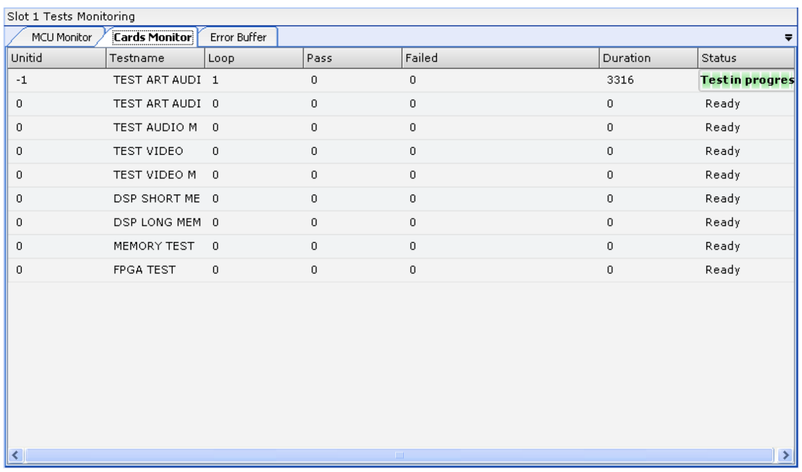


Table 23-22 *Tests Monitoring - Card Monitor Parameters*

Column	Description
Unitid	The test ID number
Testname	The name of the test
Loop	Indicates the number of times the test will repeat itself in succession.
Pass	Indicates the number of times the test passed successfully.
Failed	Indicates the number of times the test failed.
Duration	The duration of the test (in seconds).
Status	The card's current test status: *Test in Progress* or *Ready.*

Error Buffer

The Error Buffer tab displays the errors encountered during testing of the cards.

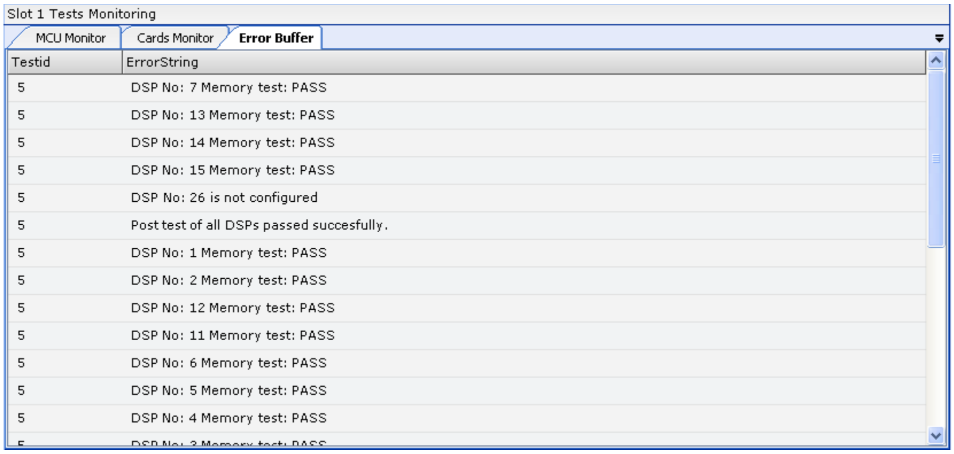


Table 23-23 *Tests Monitoring - Card Monitor Parameters*

Column	Description
Testid	The test ID number.
ErrorString	Indicates the error encountered during testing.

Temperature Thresholds

On each RMX card or there are temperature sensors that are placed near specific components on the card. In the *Hardware Monitor* you can view the properties of each card together with their temperature statuses. By right clicking on any card and viewing the cards *Properties*, the A*ctive Alarms* tab displays all the card sensors, their statuses and lists each sensor's temperature specifications. When the temperature on the cards initially rises, a fault could be triggered and can viewed in the *System Alerts, Faults List*. Load issues can arise when the system nears the maximum conference mark or high port capacity occurs on an RMX resulting in *Upper Major* or *Upper Critical* faults.

With an Upper Major alarm activation it is recommended to perform the following checks: Fans/fan tray functions, Overall System Ventilation and Filter (top, bottom & sides free and no dust) and Room temperature (cool). When no apparent cause can be found, then contact your next level of support.

However, only when the *Upper Critical* threshold is passed does the RMX system as a precaution initiate a system shutdown.

With version 7.6.1, changes have made to fan's RPM mechanism, enabling more effective responses to temperature changes on the RMX system. *Upper Major* and *Upper Critical* threshold values have sometimes also been altered, allowing for more efficient fan RPM and effective temperature management the RMX.

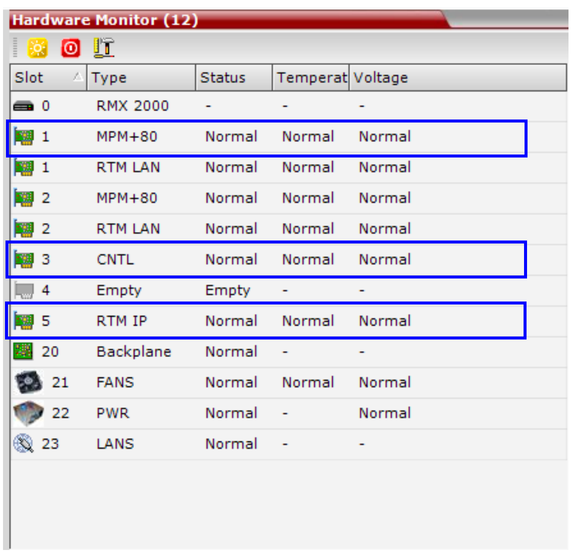


Figure 23-6*RealPresence Collaboration Server (RMX) 2000 Hardware Monitor pane*

The *Hardware Monitor* view is similar on any other RMX system.

RMX RTM-IP 1500/RTM-IP/RTM IP 4000 Card Properties

To view the RMX RTM-IP 1500/RTM-IP/RTM IP 4000 Properties:

1 In the *Hardware Monitor* pane, right-click the RTM IP entry and then select **Properties**.

> Right clicking on any RMX card will display the cards *Properties*.

2 Click **Active Alarms**.

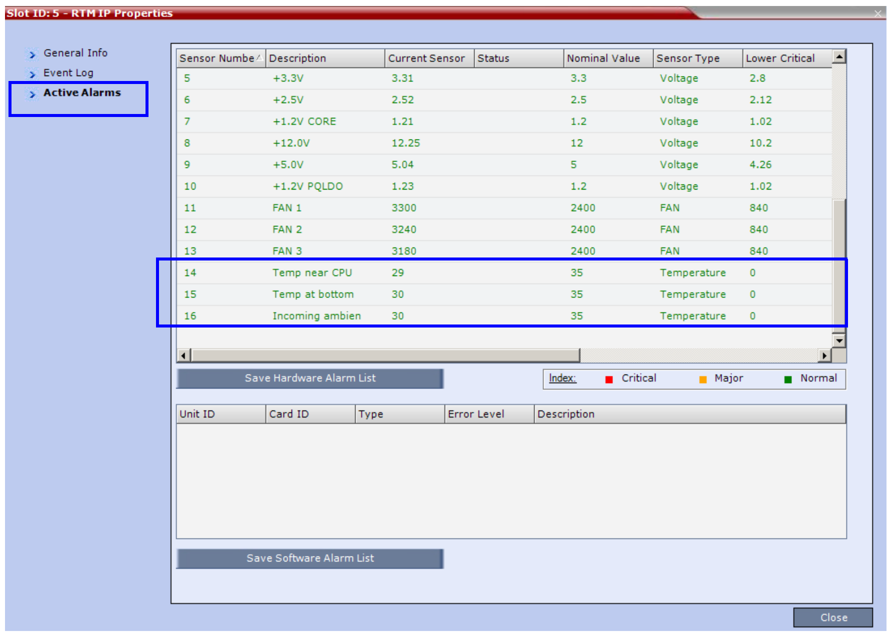


Figure 23-7 RealPresence Collaboration Server (RMX) 2000 RTM-IP Temperature Sensors

The RTM-IP is populated with 4 temperature sensors numbered: *Sensor* 14-17.

> The *Sensor* numbering and *Temperature* listings may vary on RMX systems depending on card's *Hardware Version* and *Software Version* number. The *RMX Manager* and RealPresence Collaboration Server Client software version can also affect the UI or change the look & feel.

On the *Slot ID: 5 - RTM - IP Properties,* Sensor 16 is called "*Incoming ambient*" and on the right side of the table and you can see the threshold numbers of the sensor. For example, on Sensor 14, the event "Upper Major" is activated when the temperature reaches +60° (degrees) Centigrade. The "Upper Major" event results in an alarm being triggered. Perform an overall system check. The Upper Critical event is activated when the temperature reaches a +71° (degrees) Centigrade.

CNTL Card Properties

To view the RMX CTNL Properties:

1 In the *Hardware Monitor* pane, right-click the CTNL entry and then select **Properties**.

2 Click **Active Alarms**.

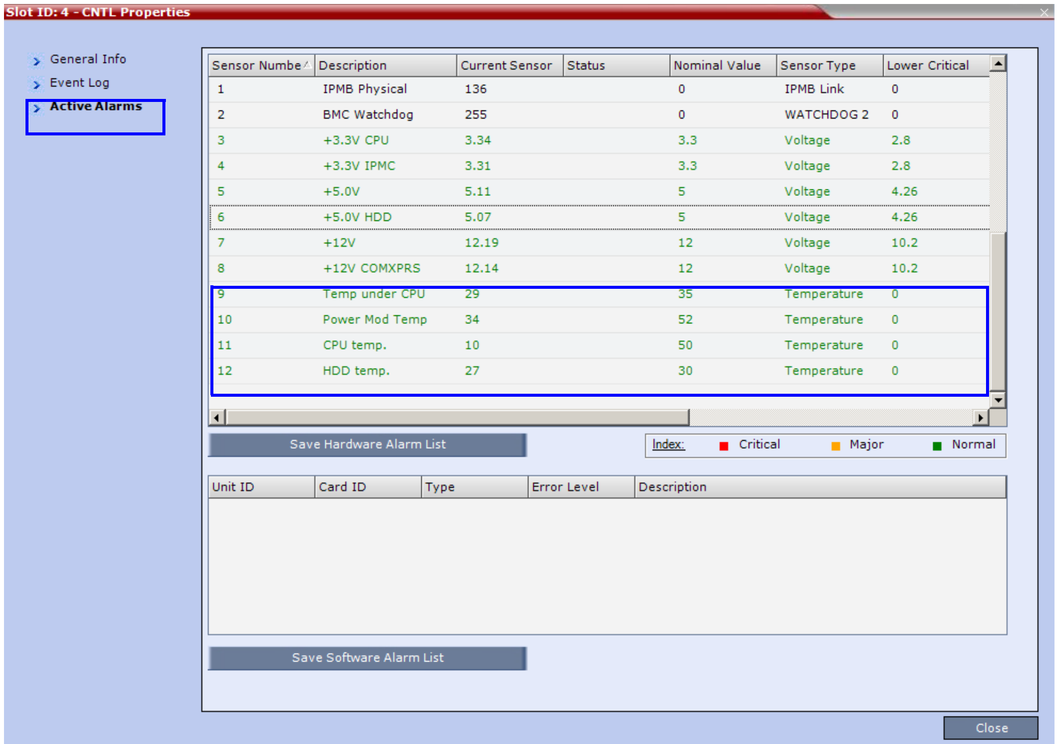


Figure 23-8RealPresence Collaboration Server (RMX) 2000 CNTL Temperature Sensors

The hottest capacity sensor on the CNTL card is sensor 10, and when this sensor reaches 70° (degrees) Centigrade, it triggers an "Upper Major" event.

The *Sensor* numbering and *Temperature* listings may vary on RMX systems depending on card's *Hardware Version* and *Software Version* number. The *RMX Manager* and RealPresence Collaboration Server Client version can also affect the UI or change the look & feel.

The "Upper Major" event results in an alarm being triggered. Perform an overall system check. If a temperature sensors reaches and passes "Upper Critical" then the Shelf Manager initiates a shutdown on the over-heated CNTL card.

MPM+ Card Properties

The MPM+ card does not support version 7.6.1 features or look & feel.

To view the MPM+ Properties:

1 In the *Hardware Monitor* pane, right-click the MPM+ entry and then select **Properties**.

Right clicking on any RMX MPM+ card will display the cards *Properties*.

2 Click **Active Alarms**.

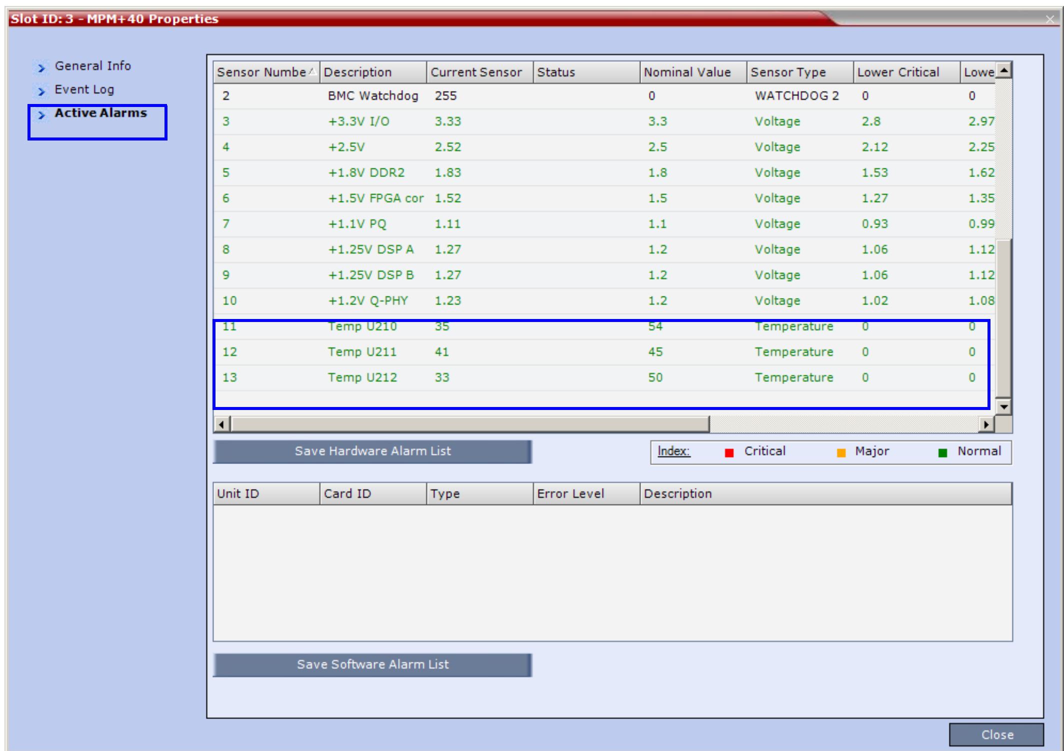


Figure 23-9RealPresence Collaboration Server (RMX) 2000 MPM+80 Properties

The MPM+80 card has 7 temperature sensors numbered: 11-17. For example, when sensor 14 reaches 70° (degrees) Centigrade, it triggers an "Upper Major" event.

The *Sensor* numbering and *Temperature* listings may vary on RMX systems depending on card's *Hardware Version* and *Software Version* number. The *RMX Manager* and RealPresence Collaboration Server Client version can also affect the UI or change the look & feel.

The "Upper Major" event results in an alarm being triggered. Perform an overall system check. If a temperature sensors reaches and passes "Upper Critical" then the Shelf Manager initiates a shutdown on the over-heated CNTL card.

MPMx Card Properties

To view the MPMx Properties:

1 In the *Hardware Monitor* pane, right-click the MPMx entry and then select **Properties**.

> Right clicking on any RMX MPMx card will display the cards *Properties*.

2 Click **Active Alarms**.

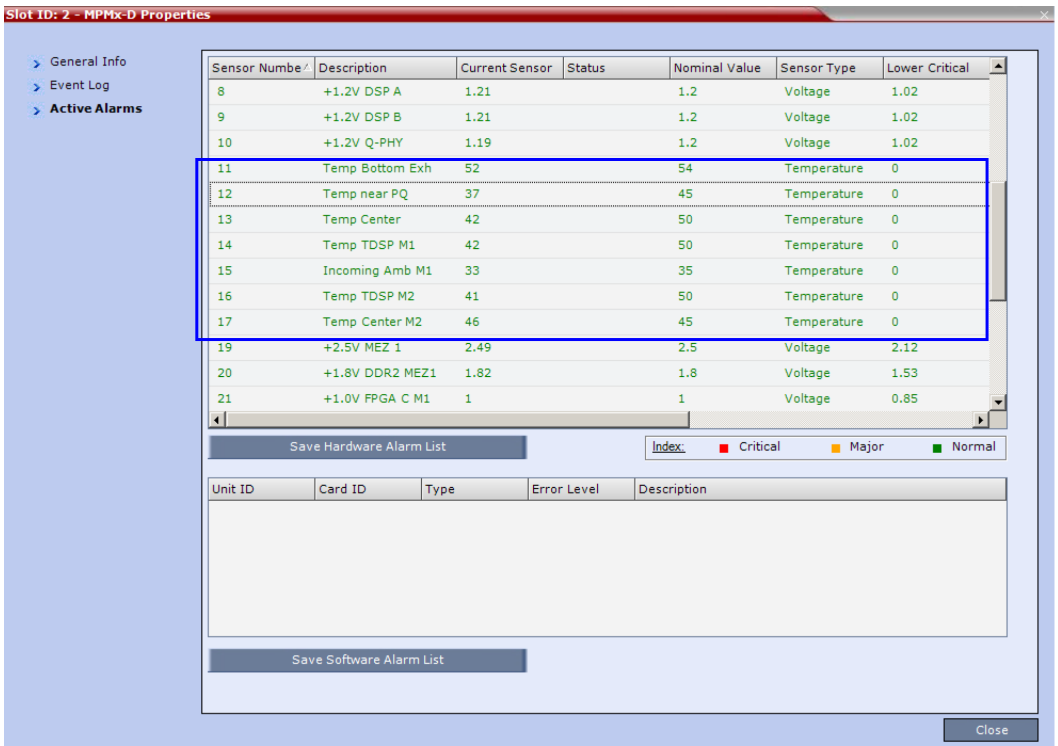


Figure 23-10*RealPresence Collaboration Server (RMX) 2000 MPMx80 Properties*

The MPMx card has 7 temperature sensors numbered: 11-17, for example, when sensor 13 reaches 70° (degrees) Centigrade, it triggers an "Upper Major" event.

> The *Sensor* numbering and *Temperature* listings may vary on RMX systems depending on card's *Hardware Version* and *Software Version* number. The *RMX Manager* and RealPresence Collaboration Server Client version can also affect the UI or change the look & feel.

The "Upper Major" event results in an alarm being triggered. Perform an overall system check. If a temperature sensors reaches and passes "Upper Critical" then the Shelf Manager initiates a shutdown on the over-heated CNTL card.

Appendix A

Disconnection Causes

If a participant was unable to connect to a conference or was disconnected from a conference, the **Connection Status** tab in the *Participant Properties* dialog box indicates the call disconnection cause. In some cases, a possible solution may be displayed.

A video participant who is unable to connect the video channels, but is able to connect as an audio only participant, is referred to as a Secondary participant. For Secondary participants, the **Connection Status** tab in the *Participant Properties* dialog box indicates the video disconnection cause. In some cases, a possible solution may be indicated.

The table below lists the call disconnection causes that can be displayed in the Call Disconnection Cause field and provides an explanation of each message

IP Disconnection Causes

Table A-1 *Call Disconnection Causes*

Disconnection Cause	Description
Disconnected by User	The user disconnected the endpoint from the conference.
Remote device did not open the encryption signaling channel	The endpoint did not open the encryption signaling channel.
Remote devices selected encryption algorithm does not match the local selected encryption algorithm	The encryption algorithm selected by the endpoint does not match the MCU's encryption algorithm.
Resources deficiency	Insufficient resources available.
Call close. Call closed by MCU	The MCU disconnected the call.
H323 call close. No port left for audio	Insufficient audio ports.
H323 call close. No port left for video	The required video ports exceed the number of ports allocated to video in fixed ports.
H323 call close. No port left for FECC	The required data ports exceed the number of ports allocated to data in fixed ports.
H323 call close. No control port left	The required control ports exceed the number of ports allocated to control data in fixed ports.
H323 call close. No port left for videocont	The required video content ports exceed the number of ports allocated to video content in fixed ports.

Table A-1 Call Disconnection Causes (Continued)

Disconnection Cause	Description
H323 call closed. Small bandwidth	The gatekeeper allocated insufficient bandwidth to the connection with the endpoint.
H323 call closed. No port left	There are no free ports left in the IP card.
Caller not registered	The calling endpoint is not registered in the gatekeeper.
H323 call closed. ARQ timeout	The endpoint sent an ARQ message to the gatekeeper, but the gatekeeper did not respond before timeout.
H323 call closed. DRQ timeout	The endpoint sent a DRQ message to the gatekeeper, but the gatekeeper did not respond before timeout.
H323 call closed. Alt Gatekeeper failure	An alternate gatekeeper failure occurred.
H323 call closed. Gatekeeper failure	A gatekeeper failure occurred.
H323 call closed. Remote busy	The endpoint was busy. (Applicable only to dial-out)
H323 call closed. Normal	The call ended normally, for example, the endpoint disconnected.
H323 call closed. Remote reject	The endpoint rejected the call.
H323 call closed. Remote unreachable	The call remained idle for more than 30 seconds and was disconnected because the destination device did not answer. Possible causes can be due to network problems, the gatekeeper could not find the endpoint's address, or the endpoint was busy or unavailable (for example, the “do not disturb” status is selected).
H323 call closed. Unknown reason	The reason for the disconnection is unknown, for example, the endpoint disconnected without giving a reason.
H323 call closed. Faulty destination address	Incorrect address format.
H323 call closed. Small bandwidth	The gatekeeper allocated insufficient bandwidth to the connection with the endpoint.
H323 call closed. Gatekeeper reject ARQ	The gatekeeper rejected the endpoint's ARQ.
H323 call closed. No port left	There are no ports left in the IP card.
H323 call closed. Gatekeeper DRQ	The gatekeeper sent a DRQ.
H323 call closed. No destination IP address	For internal use.
H323 call. Call failed prior or during the capabilities negotiation stage	The endpoint did not send its capabilities to the gatekeeper.
H323 call closed. Audio channels didn't open before timeout	The endpoint did not open the audio channel.

Table A-1 Call Disconnection Causes (Continued)

Disconnection Cause	Description
H323 call closed. Remote sent bad capability	There was a problem in the capabilities sent by the endpoint.
H323 call closed. Local capability wasn't accepted by remote	The endpoint did not accept the capabilities sent by the gatekeeper.
H323 failure	Internal error occurred.
H323 call closed. Remote stop responding	The endpoint stopped responding.
H323 call closed. Master slave problem	A People + Content cascading failure occurred.
SIP bad name	The conference name is incompatible with SIP standards.
SIP bad status	A general IP card error occurred.
SIP busy everywhere	The participant's endpoints were contacted successfully, but the participant is busy and does not wish to take the call at this time.
SIP busy here	The participant's endpoint was contacted successfully, but the participant is currently not willing or able to take additional calls.
SIP capabilities don't match	The remote device capabilities are not compatible with the conference settings.
SIP card rejected channels	The IP card could not open the media channels.
SIP client error 400	The endpoint sent a SIP Client Error 400 (Bad Request) response. The request could not be understood due to malformed syntax.
SIP client error 402	The endpoint sent a SIP Client Error 402 (Payment Required) response.
SIP client error 405	The endpoint sent a SIP Client Error 405 (Method Not Allowed) response. The method specified in the Request-Line is understood, but not allowed for the address identified by the Request-URI.
SIP client error 406	The endpoint sent a SIP Client Error 406 (Not Acceptable) resources. The remote endpoint cannot accept the call because it does not have the necessary responses. The resource identified by the request is only capable of generating response entities that have content characteristics not acceptable according to the Accept header field sent in the request.

Table A-1 Call Disconnection Causes (Continued)

Disconnection Cause	Description
SIP client error 407	The endpoint sent a SIP Client Error 407 (Proxy Authentication Required) response. The client must first authenticate itself with the proxy.
SIP client error 409	The endpoint sent a SIP Client Error 409 (Conflict) response. The request could not be completed due to a conflict with the current state of the resource.
SIP client error 411	The endpoint sent a SIP Client Error 411 (Length Required) response. The server refuses to accept the request without a defined Content Length.
SIP client error 413	The endpoint sent a SIP Client Error 413 (Request Entity Too Large) response. The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
SIP client error 414	The endpoint sent a SIP Client Error 414 (Request-URI Too Long) response. The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
SIP client error 420	The endpoint sent a SIP Client Error 420 (Bad Extension) response. The server did not understand the protocol extension specified in a Require header field.
SIP client error 481	The endpoint sent a SIP Client Error 481 (Call/ Transaction Does Not Exist) response.
SIP client error 482	The endpoint sent a SIP Client Error 482 (Loop Detected) response.
SIP client error 483	The endpoint sent a SIP Client Error 483 (Too Many Hops) response.
SIP client error 484	The endpoint sent a SIP Client Error 484 (Address Incomplete) response. The server received a request with a To address or Request-URI that was incomplete.
SIP client error 485	The endpoint sent a SIP Client Error 485 (Ambiguous) response. The address provided in the request (Request-URI) was ambiguous.
SIP client error 488	The endpoint sent a SIP Client Error 488 (Not Acceptable Here) response.

Table A-1 Call Disconnection Causes (Continued)

Disconnection Cause	Description
SIP forbidden	The SIP server rejected the request. The server understood the request, but is refusing to fulfill it.
SIP global failure 603	A SIP Global Failure 603 (Decline) response was returned. The participant's endpoint was successfully contacted, but the participant explicitly does not wish to or cannot participate.
SIP global failure 604	A SIP Global Failure 604 (Does Not Exist Anywhere) response was returned. The server has authoritative information that the user indicated in the Request-URI does not exist anywhere.
SIP global failure 606	A SIP Global Failure 606 (Not Acceptable) response was returned.
SIP gone	The requested resource is no longer available at the Server and no forwarding address is known.
SIP moved permanently	The endpoint moved permanently. The user can no longer be found at the address in the Request-URI.
SIP moved temporarily	The remote endpoint moved temporarily.
SIP not found	The endpoint was not found. The server has definitive information that the user does not exist at the domain specified in the Request-URI.
SIP redirection 300	A SIP Redirection 300 (Multiple Choices) response was returned.
SIP redirection 305	A SIP Redirection 305 (Use Proxy) response was returned. The requested resource MUST be accessed through the proxy given by the Contact field.
SIP redirection 380	A SIP Redirection 380 (Alternative Service) response was returned. The call was not successful, but alternative services are possible.
SIP remote cancelled call	The endpoint canceled the call.
SIP remote closed call	The endpoint ended the call.
SIP remote stopped responding	The endpoint is not responding.
SIP remote unreachable	The endpoint could not be reached.
SIP request terminated	The endpoint terminated the request. The request was terminated by a BYE or CANCEL request.
SIP request timeout	The request was timed out.

Table A-1 Call Disconnection Causes (Continued)

Disconnection Cause	Description
SIP server error 500	The SIP server sent a SIP Server Error 500 (Server Internal Error) response. The server encountered an unexpected condition that prevented it from fulfilling the request.
SIP server error 501	The SIP server sent a SIP Server Error 501 (Not Implemented) response. The server does not support the functionality required to fulfill the request.
SIP server error 502	The SIP server sent a SIP Server Error 502 (Bad Gateway) response. The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
SIP server error 503	The SIP server sent a SIP Server Error 503 (Service Unavailable) response. The server is temporarily unable to process the request due to a temporary overloading or maintenance of the server.
SIP server error 504	The SIP server sent a SIP Server Error 504 (Server Time-out) response. The server did not receive a timely response from an external server it accessed in attempting to process the request.
SIP server error 505	The SIP server sent a SIP Server Error 505 (Version Not Supported) response. The server does not support, or refuses to support, the SIP protocol version that was used in the request.
SIP temporarily not available	The participant's endpoint was contacted successfully but the participant is currently unavailable (e.g., not logged in or logged in such a manner as to preclude communication with the participant).
SIP remote device did not respond in the given time frame	The endpoint did not respond in the given time frame.
SIP trans error TCP Invite	A SIP Invite was sent via TCP, but the endpoint was not found.
SIP transport error	Unable to initiate connection with the endpoint.
SIP unauthorized	The request requires user authentication.
SIP unsupported media type	The server is refusing to service the request because the message body of the request is in a format not supported by the requested resource for the requested method.

ISDN Disconnection Causes

Table A-2 *ISDN Disconnection Causes*

Disconnection Cause		
Number	**Summary**	**Description**
1	*Unallocated (unassigned number)*	No route to the number exists in the ISDN network or the number was not found in the routing table. • Ensure that the number appears in the routing table. • Ensure that it is a valid number and that correct digits were dialed.
2	*No route to specified transit network (national use)*	The route specified (transit network) between the two networks does not exist.
3	*No route to destination*	No physical route to the destination number exists although the dialed number is in the routing plan. • The PRI D-Channel is malfunctioning. • Incorrect connection of the span or WAN.
4	*Send special information tone*	Return the special information tone to the calling party indicating that the called user cannot be reached.
5	*Misdialed trunk prefix (national use)*	A trunk prefix has erroneously been included in the called user number.
6	*Channel Unacceptable*	The sending entity in the call does not accept the channel most recently identified.
7	*Call awarded and being delivered in an Established channel*	The incoming call is being connected to a channel previously established for similar calls.
8	*Pre-Emption*	The call has been pre-empted.
9	*Pre-Emption – Circuit reserved for reuse*	Call is being cleared in response to user request.
16	*Normal Call Clearing*	Call cleared normally because user hung up.
17	*User Busy*	Dialed number is busy.
18	*No User Responding*	The called user has not answered the call.
19	*No Answer from User (User Alerted)*	Called user has received call alert, but has not responded within a prescribed period of time. Internal network timers may initiate this disconnection.
20	*Subscriber Absent*	User is temporarily absent from the network - as when a mobile user logs off.
21	*Call Rejected*	Called number is either busy or has compatibility issues. Supplementary service constraints in the network may also initiate the disconnection.

Table A-2 ISDN Disconnection Causes (Continued)

Disconnection Cause		
Number	**Summary**	**Description**
22	*Number Changed*	Same as Cause 1. The diagnostic field contains the new called user number. Cause 1 is used if the network does not support this cause value.
26	*Non-Selected User Clearing*	The incoming call has not been assigned to the user.
27	*Destination Out-of-Order*	Messages cannot be sent to the destination number because the span may not be active.
28	*Invalid Number Format (address incomplete)*	The Type of Number (TON) is incorrect or the number is incomplete. Network, Unknown and National numbers have different formats.
29	*Facility Rejected*	User requested supplementary service which cannot be provided by the network.
30	*Response to STATUS ENQUIRY*	A STATUS message has been received in response to a prior STATUS ENQUIRY.
31	*Normal, Unspecified*	A normal, unspecified disconnection has occurred.
34	*No Circuit/Channel Available*	No B-Channels are available for the call.
38	*Network Out-of-Order*	Network is out-of-order because due to a major malfunction.
39	*Permanent Frame Mode Connection Out-of-Service*	A permanent frame mode connection is out-of-service. This cause is part of a STATUS message.
40	*Permanent Frame Mode Connection Operational*	A permanent frame mode connection is operational. This cause is part of a STATUS message.
41	*Temporary Failure*	Minor network malfunction. Initiate call again.
42	*Switching Equipment Congestion*	High traffic has congested the switching equipment. Cause 43 is included.
43	*Access Information Discarded*	Access Information elements exceed maximum length and have been discarded. Included with Cause 42.
44	*Requested Circuit/ Channel not Available*	The requested circuit or channel is not available. Alternative circuits or channels are not acceptable.
47	*Resource Unavailable, Unspecified*	The resource is unavailable. No other disconnection cause applies.
49	*Quality of Service Not Available*	Quality of Service, as defined in Recommendation X.213, cannot be provided.
50	*Requested Facility Not Subscribed*	A supplementary service has been requested that the user is not authorized to use.

Table A-2 *ISDN Disconnection Causes (Continued)*

Disconnection Cause		
Number	**Summary**	**Description**
53	*Outgoing Calls Barred Within Closed User Group (CUG)*	Outgoing calls are not permitted for this member of the CUG.
55	*Incoming Calls Barred within CUG*	Incoming calls are not permitted for this member of the CUG.
57	*Bearer Capability Not Authorized*	A bearer capability has been requested that the user is not authorized to use.
58	*Bearer Capability Not Presently Available*	A bearer capability has been requested that the user is not presently available.
62	*Inconsistency in Designated Outgoing Access Information and Subscriber Class*	Outgoing Access and Subscriber Class information is inconsistent
63	*Service or Option Not Available, Unspecified*	The service or option is unavailable. No other disconnection cause applies.
65	*Bearer Capability Not Implemented*	The requested bearer capability is not supported.
66	*Channel Type Not Implemented*	The requested channel type is not supported.
69	*Requested Facility Not Implemented*	The requested supplementary service is not supported.
70	*Only Restricted Digital Information Bearer Capability is Available (national use)*	Unrestricted (64kb) bearer service has been requested but is not supported by the equipment sending this cause.
79	*Service or Option Not Implemented, Unspecified*	An unsupported service or unimplemented option has been requested. No other disconnection cause applies.
81	*Invalid Call Reference Value*	A message has been received which contains a call reference which is currently unassigned or not in use on the user-network interface.
82	*Identified Channel Does Not Exist*	A request has been received to use a channel which is currently inactive or does not exist.
83	*A Suspended Call Exists, but This Call Identity Does Not Exist*	A RESUME message cannot be executed by the network as a result of an unknown call identity.
84	*Call Identity in Use*	A SUSPEND message has been received with a call identity sequence that is already in use.
85	*No Call Suspended*	A RESUME message cannot be executed by the network as a result of no call suspended.

Table A-2 *ISDN Disconnection Causes (Continued)*

Disconnection Cause		
Number	**Summary**	**Description**
86	*Call Having the Requested Call Identity Has Been Cleared*	A RESUME message cannot be executed by the network as a result of the call having been cleared while suspended.
87	*User Not Member of CUG*	A CUG member was called by a user who is not a member of the CUG or a CUG call was made to a non CUG member.
88	*Incompatible Destination*	User-to-user compatibility checking procedures in a point-to-point data link have determined that an incompatibility exists between Bearer capabilities.
90	*Non-Existent CUG*	CUG does not exist.
91	*Invalid Transit Network Selection (national use)*	The transit network selection is of an incorrect format. No route (transit network) exists between the two networks.
95	*Invalid Message, Unspecified*	Invalid message received. No other disconnection cause applies.
96	*Mandatory Information Element is Missing*	A message was received with an information element missing.
97	*Message Type Non-Existent or Not Implemented*	A message was received that is of a type that is not defined or of a type that is defined but not implemented.
98	*Message is Not Compatible with the Call State, or the Message Type is Non-Existent or Not Implemented*	An unexpected message or unrecognized message incompatible with the call state has been received
99	*An Information Element or Parameter Does Not Exist or is Not Implemented*	A message was received containing elements or parameters that are not defined or of a type that is defined but not implemented.
100	*Invalid Information Element Contents*	A message other than SETUP, DISCONNECT, RELEASE, or RELEASE COMPLETE has been received which has one or more mandatory information elements containing invalid content.
101	*The Message is Not Compatible with the Call State*	A STATUS message indicating any call state except the Null state has been received while in the Null state.
102	*Recovery on Timer Expired*	An error handling procedure timer has expired.

Table A-2 ISDN Disconnection Causes (Continued)

Disconnection Cause		
Number	**Summary**	**Description**
103	*Parameter Non-Existent or Not Implemented – Passed On (national use)*	A message was received containing parameters that are not defined or of a type that is defined but not implemented.
110	*Message with Unrecognized Parameter Discarded*	A message was discarded because it contained a parameter that was not recognized.
111	*Protocol Error, Unspecified*	A protocol error has occurred. No other disconnection cause applies.
127	*Interworking, Unspecified*	An interworking call has ended.

Appendix B

Alarms and Faults

Alarms

Table B-1 *Alarms*

Alarm Code	Alarm Description
A new activation key was loaded. Reset the system.	A new activation key was loaded: Reset the MCU.
A new version was installed. Reset the system.	A new version was installed: Reset the MCU.
Alarm generated by a Central Signaling component	A system alert was generated by a component of the Central Signaling.
Alarm generated by an internal component	A system alert was generated by an internal system component.
Automatic reset is unavailable in Safe Mode	The system switches to safe mode if many resets occur during startup. To prevent additional resets, and allow the system to complete the startup process the automatic system resets are blocked.
Backup of audit files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that audit files need to be backed up.
Backup of CDR files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that CDR files need to be backed up.
Backup of log files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that log files need to be backed up.
Bios version is not compatible with Ultra Secure Mode.	The current BIOS version is not compatible with Ultra Secure Mode (ULTRA_SECURE_MODE=YES).
Card failed to switch to Ultra Secure Mode	Card failure occurred when the system was set to Ultra Secure Mode (ULTRA_SECURE_MODE=YES).
Card failure	Possible reasons for the card failure: • Resetting Card • Resetting component • Unknown shelf error • Unknown card error

Table B-1 *Alarms (Continued)*

Alarm Code	Alarm Description
Card not found	This occurs when: the system does not receive an indication about the card (since it does not exist…) usually when the card was removed from the MCU and the system did not have a chance to recalculate it resources.
Card not responding	Possible reasons for the card not responding: • No connection with MPM card. • No connection with the Switch.
Central signaling component failure	Possible explanations: • Central signaling component failure; unit type: [NonComponent\CSMngnt\CSH323\CSSIP] • Central signaling component failure; unit type: (invalid: [NonComponent\CSMngnt\CSH323\CSSIP]) • Central signaling component failure - Invalid failure type. Unit id: [id], Type: [NonComponent\CSMngnt\CSH323\CSSIP], Status: [Ok\Failed\Recovered] • Central signaling component failure - Invalid failure type
Central Signaling indicating Faulty status	Central signaling failure detected in IP Network Service.
Central Signaling indicating Recovery status	
Central Signaling startup failure	
Configuration of external database did not complete.	
Could not complete MPM Card startup procedure	Possible explanations: • Unit loading confirmation was not received. • No Media IP for this card. • Media IP Configuration confirmation was not received. • Unspecified problem.
Could not complete RTM ISDN Card startup procedure	
CPU IPMC software was not updated.	
CPU slot ID not identified	The CPU slot ID required for Ethernet Settings was not provided by the Shelf Management.
D channel cannot be established	
DEBUG mode enabled	Possible explanations: • System is running in DEBUG mode. • System DEBUG mode initiated.
DEBUG mode flags in use	System is using DEBUG CFG flags.

Table B-1 *Alarms (Continued)*

Alarm Code	Alarm Description
DMA not supported by IDE device	Possible explanations: • DMA (direct memory access) not supported by IDE device: Incompatible flash card / hard disk being used. • Flash card / hard drive are not properly connected to the board / one of the IDE channels is disconnected. • DMA was manually disabled for testing.
DNS configuration error	
DNS not configured in IP Network Service	
Encryption Server Error. Failed to generate the encryption key	FIPS 140 test failed while generating the new encryption key.
Error in external database certificate	
Error reading MCU time	Failed to read MCU time configuration file ([status]).
External NTP servers failure	Network error or configuration error
Failed to access DNS server	Failed to access DNS server.
Failed to configure the Media card IP address	Possible reasons for the failure: • Failure type: [OK Or Not supported. • Does not exist Or IP failure. • Duplicate IP Or DHCP failure. • VLAN failure Or Invalid: [status_Number].
Failed to configure the Users list in Linux	External NTP server failure: NTP server failure: [server0_ip], [server1_ip], [server2_ipStr].
Failed to connect to application server	Possible reasons for the failure: • Failed to connect to application server: • Failed to establish connection to server, url = [url].
Failed to connect to recording device	The MCU could not connect to any of the defined NTP server for synchronization due to the remote server error.
Failed to connect to SIP registrar	Cannot establish connection with SIP registrar.
Failed to create Default Profile	Possible reasons for the failure: • Failed to validate the Default Profile. • Failed to add the Default Profile.
Failed to initialize the file system	Possible reasons for the failure: • Failed to initialize the file system. • Failed to initialize the file system and create the CDR index.
Failed to open Users list file	
Failed to register with DNS server	
Failure in initialization of SNMP agent.	

Table B-1 *Alarms (Continued)*

Alarm Code	Alarm Description
Fallback version is being used	Fallback version is being used. Restore current version. Version being used: [running version]; Current version: [current version].
File error	Possible reasons for the file error: • XML file does not exist [file name]; Error no: [error number]. • Not authorized to open XML file [file name]; Error no: [error number]. • Unknown problem in opening XML file [file name]; Error no: [error number]. • Failed to parse XML file [file name].
File system scan failure	File system scan failure: Failed to scan [file system path].
File system space shortage	File system space shortage: Out of file system space in [file system path]; Free space: [free space percentage]% ([free space] Blocks) - Minimum free space required: [minimum free space percentage]% ([minimum free space] Blocks).
Gatekeeper failure	Possible reasons for the Gatekeeper failure: • Failed to register to alternate Gatekeeper. • Gatekeeper discovery state. - Check GK IP address (GUI, ping) • Gatekeeper DNS Host name not found. • Gatekeeper Registration Timeout. • Gatekeeper rejected GRQ due to invalid revision. • Gatekeeper rejected GRQ due to resource unavailability. • Gatekeeper rejected GRQ due to Terminal Exclusion. • Gatekeeper rejected GRQ due to unsupported feature. • Gatekeeper rejected GRQ. Reason 18. • Gatekeeper rejected RRQ due to Discovery Required. • Gatekeeper rejected RRQ due to duplicate alias. - Check duplicate in aliases or in prefixes • Gatekeeper rejected RRQ due to Generic Data. • Gatekeeper rejected RRQ due to invalid alias. • Gatekeeper rejected RRQ due to invalid call signaling address. • Gatekeeper rejected RRQ due to invalid endpoint ID. • Gatekeeper rejected RRQ due to invalid RAS address. • Gatekeeper rejected RRQ due to invalid revision. • Gatekeeper rejected RRQ due to invalid state.

Table B-1 *Alarms (Continued)*

Alarm Code	Alarm Description
Gatekeeper failure (cont.)	• Gatekeeper rejected RRQ due to invalid terminal alias. • Gatekeeper rejected RRQ due to resource unavailability. • Gatekeeper rejected RRQ due to Security Denial. • Gatekeeper rejected RRQ due to terminal type. • Gatekeeper rejected RRQ due to unsupported Additive Registration. • Gatekeeper rejected RRQ due to unsupported feature. • Gatekeeper rejected RRQ due to unsupported QOS transport. • Gatekeeper rejected RRQ due to unsupported transport. • Gatekeeper rejected RRQ. Full registration required. • Gatekeeper rejected RRQ. Reason 18. • Gatekeeper Unregistration State. • Registration succeeded.
GUI System configuration file is invalid xml file	The XML format of the system configuration file that contains the user interface settings is invalid.
Hard disk error	Hard disk not responding.
Insufficient resources	Insufficient resources.
Insufficient UDP Ports	
Internal System configuration during startup	System configuration during startup.
Invalid System Configuration	
IP addresses of Signaling Host and Control Unit are the same	
IP Network Service configuration modified	IP Network Service was modified. Reset the MCU.
IP Network Service deleted	IP Network Service was deleted. Reset the MCU.
IP Network Service not found	Possible explanations: • IP Service not found in the Network Services list. • m_StatusRead IpServiceList.
ISDN/PSTN Network Services configuration changed	
License not found	
Management Network not configured	
Missing Central Signaling configuration	
MPL startup failure. Authentication not received.	

Table B-1 *Alarms (Continued)*

Alarm Code	Alarm Description
MPL startup failure. Management Network configuration not received.	
No clock source	The system could not use any of the connected ISDN spans as clock source
No default ISDN/PSTN Network Service defined in ISDN/PSTN Network Services list	
No default IVR Service in IVR Services list	No default IVR Service in IVR Services list: Ensure that one conference IVR Service and one EQ IVR Service are set as default.
No IP Network Services defined	IP Network Service parameters missing.
No ISDN/PSTN Network Services defined	No ISDN/PSTN Network Services were defined or no default ISDN/PSTN Network was defined.
No License for ISDN/PSTN. Please activate the RTM ISDN card through Polycom website	
No response from Central Signaling	No connection with central signaling.
No response from RTM ISDN card	
No usable unit for audio controller	
Port configuration was modified	
Power off	
Product activation failure	
Product Type mismatch. System is restarting.	The user is alerted to a mismatch between the product type that is stored in MCU software and the product type received from another system component. In such a case the system is automatically restarted.
Recording device has disconnected unexpectedly	
Red Alarm	When a certain timeout will be reached (after startup), MCMS will go over the configured Spans. A configured Span that is related to nonexistent card – will produce a 'RED_ALARM' Alert. Similarly on HotSwap: if an RTM card (or an MPM that has an RTM extension) is removed, MCMS will go over the configured Spans. A configured Span that is related to the removed card – will produce a 'RED_ALARM' Alert.
Resource process failed to request the Meeting Room list during startup.	Without the Meeting Rooms list, the system cannot allocate the appropriate dial numbers, Conference ID etc. and therefore cannot run conferences.
Restore Failed	Restoring the system configuration has failed as the system could not locate the configuration file in the selected path, or could not open the file.
Restore Succeeded	Restoring the system configuration has succeeded. Reset the MCU.

Table B-1 *Alarms (Continued)*

Alarm Code	Alarm Description
Restoring Factory Defaults. Default system settings will be restored once Reset is completed	Default system settings will be restored once Reset is completed.
RTM ISDN card not found	RTM ISDN card is missing.
RTM ISDN card startup procedure error	The RTM ISDN card cannot complete its startup procedure (usually after system reset)
Secured SIP communication failed	
Security mode failed. Certificate has expired.	
Security mode failed. Certificate host name does not match the RMX host name.	
Security mode failed. Certificate is about to expire.	
Security mode failed. Certificate not yet valid.	
Security mode failed. Error in certificate file.	
SIP registrations limit reached	SIP registrations limit reached.
SIP TLS: Certificate has expired	The current TLS certificate files have expired and must be replaced with new files.
SIP TLS: Certificate is about to expire	The current TLS certificate files will expire shortly and will have to be replaced to ensure the communication with the OCS.
SIP TLS: Certificate subject name is not valid or DNS failed to resolve this name	This alarm is displayed if the name of the MCU in the certificate file is different from the FQDN name defined in the OCS.
SIP TLS: Failed to load or verify certificate files	This alarm indicates that the certificate files required for SIP TLS could not be loaded to the MCU. Possible causes are: • Incorrect certificate file name. Only files with the following names can be loaded to the system: rootCA.pem, pkey.pem, cert.pem and certPassword.txt • Wrong certificate file type. Only files of the following types can be loaded to the system: rootCA.pem, pkey.pem and cert.pem and certPassword.txt • The contents of the certificate file does not match the system parameters
SIP TLS: Registration handshake failure	This alarm indicates a mismatch between the security protocols of the OCS and the MCU, preventing the Registration of the MCU to the OCS.

Table B-1 *Alarms (Continued)*

Alarm Code	Alarm Description
SIP TLS: Registration server not responding	This alarm is displayed when the MCU does not receive a response from the OCS to the registration request in the expected time frame. Possible causes are: • The MCU FQDN name is not defined in the OCS pool, or is defined incorrectly. • The time frame for the expected response was too short and it will be updated with the next data refresh. The alarm may be cleared automatically the next time the data is refreshed. • The MCU FQDN name is not defined in the DNS server. Ping the DNS using the MCU FQDN name to ensure that the MCU is correctly registered to the DNS.
SIP TLS: Registration transport error	This alarm indicates that the communication with the SIP server cannot be established. Possible causes are: • Incorrect IP address of the SIP server • The SIP server listening port is other than the one defined in the system • The OCS services are stopped
SSH is enabled	
SWITCH not responding	
System Configuration modified	System configuration flags were modified. Reset the MCU.
Temperature Level - Critical	Possible explanations: • Temperature has reached a critical level. Card or if critical system element the MCU will shut down.
Temperature Level - Major	Possible explanations: • Temperature has reached a problematic level and requires attention.
The software contains patch(es)	The software contains patch(es).
The system has been configured for Ultra Secure Mode, but communication is not secured until a TLS certificate is installed and the MCU is set to Secured Communication.	Although the System Flag ULTRA_SECURE_MODE is set to YES, the Ultra Secure Mode is not fully implemented as the TLS certificate was not installed. Please install the TLS certificate and set the MCU to Secured Communication Mode to fully enable the Enhanced Security Environment.
User initiated MCU reset	MCU reset was initiated by a system user.
User Name "SUPPORT" cannot be used in Ultra Secure Mode	When Ultra Secure Mode (ULTRA_SECURE_MODE=YES) is enabled, the User Name "SUPPORT" cannot be used to define a new User.
Version upgrade is in progress	
Voltage problem	Possible reasons for the problem: • Card voltage problem. • Shelf voltage problem. • Voltage problem
Yellow Alarm	

Appendix C

CDR Fields - Unformatted File

The CDR (Call Detail Records) utility is used to retrieve conference information to a file. The CDR utility can retrieve conference information to a file in both formatted and unformatted formats.

Unformatted CDR files contain multiple records. The first record in each file contains information about the conference in general, such as the conference name and start time. The remaining records each contain information about one event that occurred during the conference, such as a participant connecting to the conference, or a user extending the length of the conference. The first field in each record identifies the event type, and this is followed by values containing information about the event. The fields are separated by commas.

Formatted files contain basically the same information as unformatted files, but with the field values replaced by descriptions. Formatted files are divided into sections, each containing information about one conference event. The first line in each section is a title describing the type of event, and this is followed by multiple lines, each containing information about the event in the form of a descriptive field name and value.

The field names and values in the formatted file will appear in the language being used for the *RealPresence Collaboration Server Web Client* user interface at the time when the CDR information is retrieved.
The value of the fields that support Unicode values, such as the info fields, will be stored in the CDR file in UTF8. The application that reads the CDR file must support Unicode.

The MCU sends the entire CDR file via API or HTTP, and the MCU or external application does the processing and sorting. The MCU ignores events that it does not recognize, that is, events written in a higher version that do not exist in the current version. Therefore, to enable compatibility between versions, instead of adding new fields to existing events, new fields are added as separate events, so as not to affect the events from older versions. This allows users with lower versions to retrieve CDR files that were created in higher versions.

This appendix describes the fields and values in the unformatted CDR records.
Although the formatted files contain basically the same information, in a few instances a single field in the unformatted file is converted to multiple lines in the formatted file, and in other cases, multiple fields in the unformatted file are combined into one line in the formatted file.

In addition, to enable compatibility for applications that were written for the MGC family, the unformatted file contains fields that were supported by the MGC family, but are not supported by the MCU, whereas these fields are omitted from the formatted file.

The Conference Summary Record

The conference summary record (the first record in the unformatted CDR file) contains the following fields:

Table C-1 *Conference Summary Record Fields*

Field	Description
File Version	The version of the CDR utility that created the file.
Conference Routing Name	The Routing Name of the conference.
Internal Conference ID	The conference identification number as assigned by the system.
Reserved Start Time	The time the conference was scheduled to start in Greenwich Mean Time (GMT). The reservation time of a reservation that was started immediately or of an ongoing conference is the same as the *Actual Start Time*.
Reserved Duration	The amount of time the conference was scheduled to last.
Actual Start Time	The actual time the conference started in GMT.
Actual Duration	The actual conference duration.
Status	The conference status code as follows: **1** - The conference is an ongoing conference. **2** - The conference was terminated by a user. **3** - The conference ended at the scheduled end time. **4** - The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. **5** - The conference never started. **6** - The conference could not start due to a problem. **8** - An unknown error occurred. **9** - The conference was terminated by a participant using DTMF codes. **Note:** If the conference was terminated by an MCU reset, this field will contain the value **1** (ongoing conference).
File Name	The name of the conference log file.
GMT Offset Sign	Indicates whether the *GMT Offset* is positive or negative. The possible values are: **0** - Offset is negative. GMT Offset will be subtracted from the GMT Time. **1** - Offset is positive. GMT Offset will be added to the GMT Time.

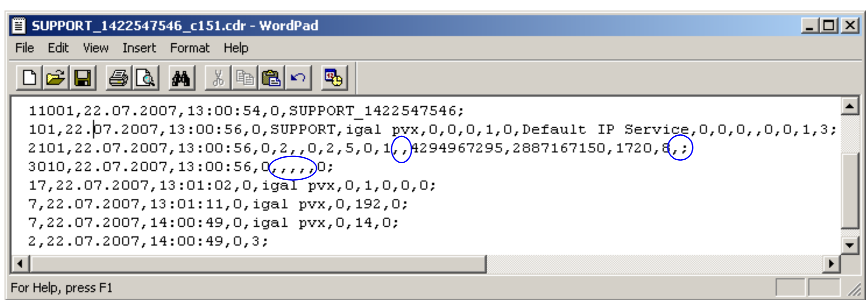
Table C-1 Conference Summary Record Fields (Continued)

Field	Description
GMT Offset	The time zone difference between Greenwich and the MCU's physical location in hours and minutes. Together with the *GMT Offset Sign* field the *GMT Offset* field is used to define the MCU local time. For example, if the *GMT Offset Sign* is 0 and *GMT Offset* is 3 hours then the time zone of the MCU's physical location is -3, which will be subtracted from the GMT time to determine the local time. However, if the *GMT Offset Sign* is 1 and *GMT Offset* is 4 hours then the time zone of the MCU's physical location is +4, which will be added to the GMT time to determine the local time.
File Retrieved	Indicates if the file has been retrieved and saved to a formatted file, as follows: **0** - No **1** - Yes

Event Records

The event records, that is, all records in the unformatted file except the first record, contain standard fields, such as the event type code and the time stamp, followed by fields that are event specific.

The event fields are separated by commas. Two consecutive commas with nothing between them (,,), or a comma followed immediately by a semi-colon (,;), indicates an empty field, as in the example below:



Standard Event Record Fields

All event records start with the following fields:

- The CDR event type code. For a list of event type codes and descriptions, refer to Table C-2, "*CDR Event Types,*" on page **C-4**.
- The event date.
- The event time.
- The structure length. This field is required for compatibility purposes, and always contains the value **0**.

Event Types

The table below contains a list of the events that can be logged in the CDR file, and indicates where to find details of the fields that are specific to that type of event.

The event code identifies the event in the unformatted CDR file, and the event name identifies the event in the formatted CDR file.

Table C-2 *CDR Event Types*

Event Code	Event Name	Description
1	*CONFERENCE START*	The conference started. For more information about the fields, see Table C-3, "*Event Fields for Event 1 - CONFERENCE START,*" on page **C-10**. **Note:** There is one CONFERENCE START event per conference. It is always the first event in the file, after the conference summary record. It contains conference details, but not participant details.
2	*CONFERENCE END*	The conference ended. For more information about the fields, see Table C-8, "*Event Fields for Event 2 - CONFERENCE END,*" on page **C-15**. **Note:** There is one CONFERENCE END event per conference, and it is always the last event in the file.
3	*ISDN/PSTN CHANNEL CONNECTED*	An ISDN/PSTN channel connected. For more information about the fields, see Table C-9, "*Event fields for Event 3 - ISDN/PSTN CHANNEL CONNECTED,*" on page **C-15**.
4	*ISDN/PSTN CHANNEL DISCONNECTED*	An ISDN/PSTN channel disconnected. For more information about the fields, see Table C-10, "*Event fields for Event 4 - ISDN/PSTN CHANNEL DISCONNECTED,*" on page **C-17**.
5	*ISDN/PSTN PARTICIPANT CONNECTED*	An ISDN/PSTN participant connected to the conference. For more information about the fields, see Table C-11, "*Event fields for Event 5 - ISDN/PSTN PARTICIPANT CONNECTED,*" on page **C-17**.
7	*PARTICIPANT DISCONNECTED*	A participant disconnected from the conference. For more information about the fields, see Table C-12, "*Event Fields for Event 7 - PARTICIPANT DISCONNECTED,*" on page **C-19**.

Table C-2 CDR Event Types (Continued)

Event Code	Event Name	Description
10	*DEFINED PARTICIPANT*	Information about a defined participant, that is, a participant who was added to the conference before the conference started. For more information about the fields, see Table C-14, "*Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT,"* on page **C-20**. **Note:** There is one event for each participant defined before the conference started.
15	*H323 CALL SETUP*	Information about the IP address of the participant. For more information about the fields, see Table C-17, "*Event fields for Event 15 - H323 CALL SETUP,"* on page **C-24**.
17	*H323 PARTICIPANT CONNECTED*	An H.323 participant connected to the conference. For more information about the fields, see Table C-18, "*Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED,"* on page **C-25**.
18	*NEW UNDEFINED PARTICIPANT*	A new undefined participant joined the conference. For more information about the fields, see Table C-19, "*Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT,"* on page **C-26**.
20	*BILLING CODE*	A billing code was entered by a participant using DTMF codes. For more information about the fields, see Table C-21, "*Event Fields for Event 20 - BILLING CODE,"* on page **C-29**.
21	*SET PARTICIPANT DISPLAY NAME*	A user assigned a new name to a participant, or an end point sent its name. For more information about the fields, see Table C-22, "*Event Fields for Event 21 - SET PARTICIPANT DISPLAY NAME,"* on page **C-30**.
22	*DTMF CODE FAILURE*	An error occurred when a participant entered a DTMF code. For more information about the fields, see Table C-23, "*Event Fields for Event 22 - DTMF CODE FAILURE,"* on page **C-30**.
23	*SIP PARTICIPANT CONNECTED*	A SIP participant connected to the conference. For more information about the fields, see Table C-18, "*Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED,"* on page **C-25**.
26	*RECORDING LINK*	A recording event, such as recording started or recording resumed, occurred. For more information about the fields, see Table C-24, "*Event fields for Event 26 - RECORDING LINK,"* on page **C-30**.

Table C-2 CDR Event Types (Continued)

Event Code	Event Name	Description
28	*SIP PRIVATE EXTENSIONS*	Contains SIP Private Extensions information. For more information about the fields, see Table C-25, “*Event Fields for Event 28 - SIP PRIVATE EXTENSIONS,”* on page **C-31**.
30	*GATEKEEPER INFORMATION*	Contains the gatekeeper caller ID, which makes it possible to match the CDR in the gatekeeper and in the MCU. For more information about the fields, see Table C-26, “*Event Fields for Event 30 - GATEKEEPER INFORMATION,”* on page **C-31**.
31	*PARTICIPANT CONNECTION RATE*	Information about the line rate of the participant connection. This event is added to the CDR file each time the endpoint changes its connection bit rate. For more information about the fields, see Table C-27, “*Event fields for Event 31 - PARTICIPANT CONNECTION RATE,”* on page **C-31**.
32	*EVENT NEW UNDEFINED PARTY CONTINUE IPV6 ADDRESS*	Information about the IPv6 address of the participant’s endpoint.
33	*PARTY CHAIR UPDATE*	Participants connect to the conferences as standard participants and they are designated as chairpersons either by entering the chairperson password during the IVR session upon connection, or while participating in the conference using the appropriate DTM code. For more information about the fields, see see “*Event fields for Event 33 - PARTY CHAIR UPDATE”* on page **C-32**.
34	*PARTICIPANT MAXIMUM USAGE INFORMATION*	This event includes information of the maximum line rate, maximum resolution and maximum frame rate used by H.323 or SIP participant during the conference.
35	*SVC SIP PARTICIPANT CONNECTED*	An SVC user connected over SIP. For more information about the fields, see Table C-31, “*Event Fields for Event 35 - SVC SIP PARTICIPANT CONNECTED,”* on page **C-33**.
100	*USER TERMINATE CONFERENCE*	A user terminated the conference. For more information about the fields, see Table C-32, “*Event Fields for Event 100 - USER TERMINATE CONFERENCE,”* on page **C-33**.

Table C-2 *CDR Event Types (Continued)*

Event Code	Event Name	Description
101	*USER ADD PARTICIPANT*	A user added a participant to the conference during the conference. For more information about the fields, see Table C-14, "*Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT,"* on page **C-20**.
102	*USER DELETE PARTICIPANT*	A user deleted a participant from the conference. For more information about the fields, see Table C-33, "*Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT,"* on page **C-34**.
103	*USER DISCONNECT PARTICIPANT*	A user disconnected a participant. For more information about the fields, see Table C-33, "*Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT,"* on page **C-34**.
104	*USER RECONNECT PARTICIPANT*	A user reconnected a participant who was disconnected from the conference. For more information about the fields, see Table C-33, "*Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT,"* on page **C-34**.
105	*USER UPDATE PARTICIPANT*	A user updated the properties of a participant during the conference. For more information about the fields, see Table C-14, "*Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT,"* on page **C-20**.
106	*USER SET END TIME*	A user modified the conference end time. For more information about the fields, see Table C-34, "*Event Fields for Event 106 - USER SET END TIME,"* on page **C-34**.
107	*OPERATOR MOVE PARTY FROM CONFERENCE*	The participant moved from an Entry Queue to the destination conference or between conferences. For more information about the fields, see Table C-35, "*Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY,"* on page **C-34**.
108	*OPERATOR MOVE PARTY TO CONFERENCE*	The MCU User moved the participant from an ongoing conference to another conference. For more information, see Table C-36, "*Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE,"* on page **C-34**.

Table C-2 *CDR Event Types (Continued)*

Event Code	Event Name	Description
109	*OPERATOR ATTEND PARTY*	The MCU User moved the participant to the Operator conference. For more information, see Table C-35, "*Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY,"* on page **C-34**.
111	*OPERATOR BACK TO CONFERENCE PARTY*	The MCU User moved the participant back to his Home (source) conference. For more information, see Table C-37, "*Event Fields for Event 111 - OPERATOR BACK TO CONFERENCE PARTY,"* on page **C-38**.
112	*OPERATOR ATTEND PARTY TO CONFERENCE*	The MCU User moved the participant from the Operator conference to another conference. For more information, see Table C-36, "*Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE,"* on page **C-34**.
1001	*NEW UNDEFINED PARTICIPANT CONTINUE 1*	Additional information about a NEW UNDEFINED PARTICIPANT event. For more information about the fields, see Table C-20, "*Event Fields for Event 1001 - NEW UNDEFINED PARTY CONTINUE 1,"* on page **C-29**.
2001	*CONFERENCE START CONTINUE 1*	Additional information about a CONFERENCE START event. For more information about the fields, see Table C-4, "*Event Fields for Event 2001 - CONFERENCE START CONTINUE 1,"* on page **C-12**.
2007	*PARTICIPANT DISCONNECTED CONTINUE 1*	Additional information about a PARTICIPANT DISCONNECTED event. For more information about the fields, see Table C-13, "*Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1,"* on page **C-19**.
2010	*DEFINED PARTICIPANT CONTINUE 1*	Additional information about a DEFINED PARTICIPANT event. For more information about the fields, see Table C-15, "*Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1,"* on page **C-22**.
2011	*RESERVED PARTICIPANT CONTINUE PV6 ADDRESS*	Additional information about a DEFINED PARTICIPANT event that includes the IPv6 addressing of the defined participant. For more details, see "*Event Fields for Events 2011, 2012, and 2016"* on page **C-38**.

Table C-2 *CDR Event Types (Continued)*

Event Code	Event Name	Description
2012	*RESERVED PARTICIPANT CONTINUE 2*	Additional information about a DEFINED PARTICIPANT event. For more information about the fields, see Table C-16, "*Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2,"* on page **C-24**.
2101	*USER ADD PARTICIPANT CONTINUE 1*	Additional information about a USER ADD PARTICIPANT event. For more information about the fields, see Table C-15, "*Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1,"* on page **C-22**.
2102	*USER ADD PARTICIPANT CONTINUE 2*	Additional information about a USER ADD PARTICIPANT event. For more information about the fields, see Table C-16, "*Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2,"* on page **C-24**.
2105	*USER UPDATE PARTICIPANT CONTINUE 1*	Additional information about a USER UPDATE PARTICIPANT event. For more information about the fields, see Table C-15, "*Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1,"* on page **C-22**.
2106	*USER UPDATE PARTICIPANT CONTINUE 2*	Additional information about a USER UPDATE PARTICIPANT event. For more information about the fields, see Table C-16, "*Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2,"* on page **C-24**.
3010	*PARTICIPANT INFORMATION*	The contents of the participant information fields. For more information about the fields, see Table C-39, "*Event Fields for Event 3010 - PARTICIPANT INFORMATION,"* on page **C-39**.

Table C-2 *CDR Event Types (Continued)*

Event Code	Event Name	Description
5001	*CONFERENCE START CONTINUE 4*	Additional information about a CONFERENCE START event. For more information about the fields, see Table C-5, "*Event Fields for Event 5001 - CONFERENCE START CONTINUE 4,*" on page **C-14**. **Note:** An additional CONFERENCE START CONTINUE 4 event will be written to the CDR each time the value of one of the following conference fields is modified: • Conference Password • Chairperson Password • Info1, Info2 or Info3 • Billing Info These additional events will only contain the value of the modified field.
6001	*CONFERENCE START CONTINUE 5*	Additional information about a CONFERENCE START event. For more information about the fields, see Table C-6, "*Event Fields for Event 6001 - CONFERENCE START CONTINUE 5,*" on page **C-15**.
11001	*CONFERENCE START CONTINUE 10*	Additional information about a CONFERENCE START event. This event contains the Display Name. For more information about the fields, see Table C-7, "*Event Fields for Event 11001 - CONFERENCE START CONTINUE 10,*" on page **C-15**.

This list only includes events that are supported by the MCU. For a list of MGC Manager events that are not supported by the RMX, see "*MGC Manager Events that are not Supported by the MCU*" on page **C-42**.

Event Specific Fields

The following tables describe the fields which are specific to each type of event.

Some fields that were supported by the MGC Manager, are not supported by the MCU. In addition, for some fields the MCU has a fixed value, whereas the MGC Manager supported multiple values. For more information about the MGC Manager fields and values, see the *MGC Manager User's Guide Volume II*, *Appendix A*.

Table C-3 *Event Fields for Event 1 - CONFERENCE START*

Field	Description
Dial-Out Manually	Indicates whether the conference was a dial-out manually conference or not. Currently the only value is: **0** - The conference was *not* a dial-out manually conference, that is, the MCU initiates the communication with dial-out participants, and the user does not need to connect them manually.

Table C-3 Event Fields for Event 1 - CONFERENCE START (Continued)

Field	Description
Auto Terminate	Indicates whether the conference was set to end automatically if no participant joins the conference for a predefined time period after the conference starts, or if all participants disconnect from the conference and the conference is empty for a predefined time period. Possible values are: **0** - The conference was *not* set to end automatically. **1** - The conference was set to end automatically.
Line Rate	The conference line rate, as follows: **0** - 64 kbps **6** - 384 kbps **12** - 1920 kbps **13** - 128 kbps **15** - 256 kbps **23** - 512 kbps **24** - 768 kbps **26** - 1152 kbps **29** - 1472 kbps **32** - 96 kbps
Line Rate (cont.)	**33** - 1024 kbps **34** - 4096 kbps
Restrict Mode	Not supported. Always contains the value **0**.
Audio Algorithm	The audio algorithm. Currently the only value is: **255** - Auto
Video Session	The video session type. Currently the only value is: **3** - Continuous Presence
Video Format	The video format. Currently the only value is: **255** - Auto
CIF Frame Rate	The CIF frame rate. Currently the only value is: **255** -Auto
QCIF Frame Rate	The QCIF frame rate: Currently the only value is: **255** - Auto
LSD Rate	Not supported. Always contains the value **0**.
HSD Rate	Not supported. Always contains the value **0**.

Table C-3 *Event Fields for Event 1 - CONFERENCE START (Continued)*

Field	Description
T120 Rate	Not supported. Always contains the value **0**.

Table C-4 *Event Fields for Event 2001 - CONFERENCE START CONTINUE 1*

Field	Description
Audio Tones	Not supported. Always contains the value **0**.
Alert Tone	Not supported. Always contains the value **0**.
Talk Hold Time	The minimum time that a speaker has to speak to become the video source. The value is in units of 0.01 seconds. Currently the only value is **150**, which indicates a talk hold time of 1.5 seconds.
Audio Mix Depth	The maximum number of participants whose audio can be mixed. Currently the only value is **5**.
Operator Conference	Not supported. Always contains the value **0**.
Video Protocol	The video protocol. Currently the only value is: **255** - Auto
Meet Me Per Conference	Indicates the Meet Me Per Conference setting. Currently the only value is: **1** - The Meet Me Per Conference option is enabled, and dial-in participants can join the conference by dialing the dial-in number.
Number of Network Services	Not supported. Always contains the value **0**.
Chairperson Password	The chairperson password for the conference. An empty field “” means that no chairperson password was assigned to the conference.
Chair Mode	Not supported. Always contains the value **0**.
Cascade Mode	The cascading mode. Currently the only value is: **0** - None
Master Name	Not supported. This field remains empty.

Table C-4 Event Fields for Event 2001 - CONFERENCE START CONTINUE 1 (Continued)

Field	Description
Minimum Number of Participants	The number of participants for which the system reserved resources. Additional participants may join the conference without prior reservation until all the resources are utilized. Currently the only value is **0**.
Allow Undefined Participants	Indicates whether or not undefined dial-in participants can connect to the conference. Currently the only value is: **1** - Undefined participants can connect to the conference
Time Before First Participant Joins	**Note:** This field is only relevant if the Auto Terminate option is enabled. Indicates the number of minutes that should elapse from the time the conference starts, without any participant connecting to the conference, before the conference is automatically terminated by the MCU.
Time After Last Participant Quits	**Note:** This field is only relevant if the Auto Terminate option is enabled. Indicates the number of minutes that should elapse after the last participant has disconnected from the conference, before the conference is automatically terminated by the MCU.
Conference Lock Flag	Not supported. Always contains the value **0**.
Maximum Number of Participants	The maximum number of participants that can connect to the conference at one time. The value **65535** (auto) indicates that as many participants as the MCU's resources allow can connect to the conference, up to the maximum possible for the type of conference.
Audio Board ID	Not supported. Always contains the value **65535**.
Audio Unit ID	Not supported. Always contains the value **65535**.
Video Board ID	Not supported. Always contains the value **65535**.
Video Unit ID	Not supported. Always contains the value **65535**.
Data Board ID	Not supported. Always contains the value **65535**.
Data Unit ID	Not supported. Always contains the value **65535**.
Message Service Type	The Message Service type. Currently the only value is: **3** - IVR
Conference IVR Service	The name of the IVR Service assigned to the conference. **Note:** If the name of the IVR Service contains more than 20 characters, it will be truncated to 20 characters.

Table C-4 Event Fields for Event 2001 - CONFERENCE START CONTINUE 1 (Continued)

Field	Description
Lecture Mode Type	Indicates the type of Lecture Mode, as follows: **0** - None **1** - Lecture Mode **3** - Presentation Mode
Lecturer	**Note:** This field is only relevant if the Lecture Mode Type is Lecture Mode. The name of the participant selected as the conference lecturer.
Time Interval	**Note:** This field is only relevant if Lecturer View Switching is enabled. The number of seconds a participant is to be displayed in the lecturer window before switching to the next participant. Currently the only value is **15**.
Lecturer View Switching	**Note:** This field is only relevant when Lecture Mode is enabled. Indicates the lecturer view switching setting, as follows: **0** - Automatic switching between participants is disabled. **1** - Automatic switching between participants is enabled.
Audio Activated	Not supported. Always contains the value **0**.
Lecturer ID	Not supported. Always contains the value **4294967295**.

Table C-5 Event Fields for Event 5001 - CONFERENCE START CONTINUE 4

Field	Description
Note: When this event occurs as the result of a change to the value of one of the event fields, the event will only contain the value of the modified field. All other fields will be empty.	
Conference ID	The conference ID.
Conference Password	The conference password. An empty field "" means that no conference password was assigned to the conference.
Chairperson Password	The chairperson password. An empty field "" means that no chairperson password was assigned to the conference.
Info1 *Info2* *Info3*	The contents of the conference information fields. These fields enable users to enter general information for the conference, such as the company name, and the contact person's name and telephone number. The maximum length of each field is 80 characters.
Billing Info	The billing code.

Table C-6 *Event Fields for Event 6001 - CONFERENCE START CONTINUE 5*

Field	Description
Encryption	Indicates the conference encryption setting, as follows: **0** - The conference is *not* encrypted. **1** - The conference is encrypted.

Table C-7 *Event Fields for Event 11001 - CONFERENCE START CONTINUE 10*

Field	Description
Display Name	The Display Name of the conference.

Table C-8 *Event Fields for Event 2 - CONFERENCE END*

Field	Description
Conference End Cause	Indicates the reason for the termination of the conference, as follows: **1** - The conference is an ongoing conference or the conference was terminated by an MCU reset. **2** - The conference was terminated by a user. **3** - The conference ended at the scheduled end time. **4** - The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. **5** - The conference never started. **6** - The conference could not start due to a problem. **8** - An unknown error occurred. **9** - The conference was terminated by a participant using DTMF codes.

Table C-9 *Event fields for Event 3 - ISDN/PSTN CHANNEL CONNECTED*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Channel ID	The channel identifier.
Number of Channels	The number of channels being connected for this participant.
Connect Initiator	Indicates who initiated the connection, as follows: **0** - MCU **1** - Participant **Any other number** - Unknown

Table C-9 Event fields for Event 3 - ISDN/PSTN CHANNEL CONNECTED (Continued)

Field	Description
Call Type	The call type, as follows: **68** - 56 KBS data call **72** - 1536kbs data call (PRI only) **75** - 56 KBS data call **77** - Modem data service **79** - 384kbs data call (PRI only) **86** - Normal voice call
Network Service Program	The Network Service program, as follows: **0** - None **1** - ATT_SDN or NTI_PRIVATE **3** - ATT_MEGACOM or NTI_OUTWATS **4** - NTI FX **5** - NTI TIE TRUNK **6** - ATT ACCUNET **8** - ATT 1800 **16** - NTI_TRO
Preferred Mode	The value of the preferred/exclusive field for B channel selection (the PRF mode), as follows: **0** - None **1** - Preferred **2** - Exclusive For more details refer to the Q.931 standard.
Calling Participant Number Type	The type of calling number, as follows: **0** - Unknown, default **1** - International **2** - National **3** - Network specific **4** - Subscriber **6** - Abbreviated
Calling Participant Number Plan	The calling participant number plan. **0** - Unknown **1** - ISDN/PSTN **9** - Private
Calling Participant Presentation Indicator	The calling participant presentation indicator, as follows: **0** - Presentation allowed, default **1** - Presentation restricted **2** - Number not available **255** - Unknown
Calling Participant Screening Indicator	The calling participant screening indicator, as follows: **0** - Participant not screened, default **1** - Participant verification succeeded **2** - Participant verification failed **3** - Network provided **255** - Unknown

Table C-9 *Event fields for Event 3 - ISDN/PSTN CHANNEL CONNECTED (Continued)*

Field	Description
Calling Participant Phone Number	The telephone number used for dial-in.
Called Participant Number Type	The type of number called, as follows: **0** - Unknown, default **1** - International **2** - National **3** - Network specific **4** - Subscriber **6** - Abbreviated
Called Participant Number Plan	The called participant number plan, as follows: **0** - Unknown **1** - ISDN/PSTN **9** - Private
Called Participant Phone Number	The telephone number used for dial-out.

Table C-10 *Event fields for Event 4 - ISDN/PSTN CHANNEL DISCONNECTED*

Field	Description
Participant Name	The participant name.
Participant ID	The identification number assigned to the participant by the MCU.
Channel ID	The channel identifier.
Disconnect Initiator	Indicates who initiated the disconnection, as follows: **0** - MCU **1** - Participant **Any other number** - Unknown
Disconnect Coding Standard	The disconnection cause code standard. For values and explanations, see the Q.931 Standard.
Disconnect Location	The disconnection cause location. For values and explanations, see the Q.931 Standard.
Q931 Disconnection Cause	The disconnection cause value. For values and explanations, see the Q.931 Standard.

Table C-11 *Event fields for Event 5 - ISDN/PSTN PARTICIPANT CONNECTED*

Field	Description
Participant Name	The name of the participant.

Table C-11 Event fields for Event 5 - ISDN/PSTN PARTICIPANT CONNECTED (Continued)

Field	Description
Participant ID	The identification number assigned to the participant by the MCU.
Participant Status	The participant status, as follows: **0** - Idle **1** - Connected **2** - Disconnected **3** - Waiting for dial-in **4** - Connecting **5** - Disconnecting **6** - Partially connected. Party has completed H.221 capability exchange **7** - Deleted by a user **8** - Secondary. The participant could not connect the video channels and is connected via audio only **10** - Connected with problem **11** - Redialing
Remote Capabilities	**Note:** This field is only relevant to ISDN video participants. The remote capabilities in H.221 format.
Remote Communication Mode	**Note:** This field is only relevant to ISDN video participants. The remote communication mode in H.221 format.
Secondary Cause	**Note:** This field is only relevant to ISDN video participants and only if the Participant Status is Secondary. The cause for the secondary connection (not being able to connect the video channels), as follows: **0** - Default **11** - The incoming video parameters are not compatible with the conference video parameters **12** - H.323 card failure **13** - The conference video settings are not compatible with the endpoint capabilities **14** - The new conference settings are not compatible with the endpoint capabilities

Table C-11 Event fields for Event 5 - ISDN/PSTN PARTICIPANT CONNECTED (Continued)

Field	Description
Secondary Cause (cont.)	**15** - Video stream violation due to incompatible annexes or other discrepancy. **16** - Inadequate video resources **17** - When moved to a Transcoding or Video Switching conference, the participant's video capabilities are not supported by the video cards **18** - Video connection could not be established **24** - The endpoint closed its video channels **25** - The participant video settings are not compatible with the conference protocol **26** - The endpoint could not re-open the video channel after the conference video mode was changed **27** - The gatekeeper approved a lower bandwidth than requested **28** - Video connection for the SIP participant is temporarily unavailable **29** - AVF problem. Insufficient bandwidth. **30** - H2.39 bandwidth mismatch **255** - Other

Table C-12 Event Fields for Event 7 - PARTICIPANT DISCONNECTED

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Call Disconnection Cause	The disconnection cause. For more information about possible values, see Table C-40, "*Disconnection Cause Values,"* on page **C-39**.
Q931 Disconnect Cause	If the disconnection cause is "No Network Connection" or "Participant Hang Up", then this field indicates the Q931 disconnect cause.

Table C-13 Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1

Field	Description
Rx Synchronization Loss	The number of times that the general synchronization of the MCU was lost.
Tx Synchronization Loss	The number of times that the general synchronization of the participant was lost.
Rx Video Synchronization Loss	The number of times that the synchronization of the MCU video unit was lost.
Tx Video Synchronization Loss	The number of times that the synchronization of the participant video was lost.

Table C-13 *Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1*

Field	Description
Mux Board ID	Not supported. Always contains the value **0**.
Mux Unit ID	Not supported. Always contains the value **0**.
Audio Codec Board ID	Not supported. Always contains the value **0**.
Audio Codec Unit ID	Not supported. Always contains the value **0**.
Audio Bridge Board ID	Not supported. Always contains the value **0**.
Audio Bridge Unit ID	Not supported. Always contains the value **0**.
Video Board ID	Not supported. Always contains the value **0**.
Video Unit ID	Not supported. Always contains the value **0**.
T.120 Board ID	Not supported. Always contains the value **0**.
T.120 Unit ID	Not supported. Always contains the value **0**.
T.120 MCS Board ID	Not supported. Always contains the value **0**.
T.120 MCS Unit ID	Not supported. Always contains the value **0**.
H.323 Board ID	Not supported. Always contains the value **0**.
H323 Unit ID	Not supported. Always contains the value **0**.

Table C-14 *Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT*

Field	Description
User Name	The login name of the user who added the participant to the conference, or updated the participant properties.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Table C-14 *Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT (Continued)*

Field	Description
Dialing Direction	The dialing direction, as follows: **0** - Dial-out **5** - Dial-in
Bonding Mode	Not supported. Always contains the value **0**.
Number Of Channels	**Note:** This field is only relevant to ISDN/PSTN participants. The number of channels being connected for this participant.
Net Channel Width	Not supported. Always contains the value **0**.
Network Service Name	The name of the Network Service. An empty field “” indicates the default Network Service.
Restrict	Not supported. Always contains the value **0**.
Audio Only	Indicates the participant’s Audio Only setting, as follows: **0** - The participant is *not* an Audio Only participant **1** - The participant is an Audio Only participant **255** - Unknown
Default Number Type	**Note:** This field is only relevant to ISDN/PSTN participants. The type of telephone number, as follows: **0** - Unknown **1** - International **2** - National **3** - Network specific **4** - Subscriber **6** - Abbreviated **255** - Taken from Network Service, default **Note:** For dial-in participants, the only possible value is: **255** - Taken from Network Service
Net Sub-Service Name	Not supported. This field remains empty.
Number of Participant Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The number of participant phone numbers. In a dial-in connection, the participant phone number is the CLI (Calling Line Identification) as identified by the MCU. In a dial-out connection, participant phone numbers are the phone numbers dialed by the MCU for each participant channel.

Table C-14 Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT (Continued)

Field	Description
Number of MCU Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The number of MCU phone numbers. In a dial-in connection, the MCU phone number is the number dialed by the participant to connect to the MCU. In a dial-out connection, the MCU phone number is the MCU (CLI) number as seen by the participant.
Party and MCU Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. No, one or more fields, one field for each participant and MCU phone number. The participant phone numbers are listed first, followed by the MCU phone numbers.
Identification Method	**Note:** This field is only relevant to dial-in participants. The method by which the destination conference is identified, as follows: **1** - Called phone number, IP address or alias **2** - Calling phone number, IP address or alias
Meet Me Method	**Note:** This field is only relevant to dial-in participants. The meet-me per method. Currently the only value is: **3** - Meet-me per participant

Table C-15 Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1

Field	Description
Network Type	The type of network between the participant and the MCU, as follows: **0** - ISDN/PSTN **2** - H.323 **5** - SIP
H.243 Password	Not supported. This field remains empty.
Chair	Not supported. Always contains the value **0**.
Video Protocol	The video protocol used by the participant, as follows: **1** - H.261 **2** - H.263 **4** - H.264 **255** - Auto
Broadcasting Volume	The broadcasting volume assigned to the participant. The value is between **1** (lowest) and **10** (loudest). Each unit movement increases or decreases the volume by **3 dB**.

Table C-15 *Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1*

Field	Description
Undefined Participant	Indicates whether are not the participant is an undefined participant, as follows: **0** - The participant is *not* an undefined participant. **2** - The participant is an undefined participant.
Node Type	The node type, as follows: **0** - MCU **1** - Terminal
Bonding Phone Number	**Note:** This field is only relevant to ISDN/PSTN participants. The phone number for Bonding dial-out calls. Bonding is a communication protocol that aggregates from two up to thirty 64 Kbps B channels together, to look like one large bandwidth channel.
Video Bit Rate	The video bit rate in units of kilobits per second. A value of **4294967295** denotes auto, and in this case, the rate is computed by the MCU.
IP Address	**Note:** This field is only relevant to IP participants. The IP address of the participant. An address of **4294967295** indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Signaling Port	**Note:** This field is only relevant to IP participants. The signaling port used for participant connection.
H.323 Participant Alias Type/SIP Participant Address Type	**Note:** This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: **7** - E164 **8** - H.323 ID **13** - Email ID **14** - Participant number For SIP participants, the address type, as follows: **1** - SIP URI **2** - Tel URL
H.323 Participant Alias Name/SIP Participant Address	**Note:** This field is only relevant to IP participants. For H.323 participants: The participant alias. The alias may contain up to 512 characters. For SIP participants: The participant address. The address may contain up to 80 characters.

Table C-16 *Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2*

Field	Description
Encryption	Indicates the participant's encryption setting as follows: **0** - The participant is *not* encrypted. **1** - The participant is encrypted. **2** - Auto. The conference encryption setting is applied to the participant.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Table C-17 *Event fields for Event 15 - H323 CALL SETUP*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Connect Initiator	Indicates who initiated the connection, as follows: **0** - MCU **1** - Remote participant **Any other number** - Unknown
Min Rate	The minimum line rate used by the participant. The data in this field should be ignored. For accurate rate information, see CDR event 31.
Max Rate	The maximum line rate achieved by the participant. The data in this field should be ignored. For accurate rate information, see CDR event 31.
Source Party Address	The IP address of the calling participant. A string of up to 255 characters.
Destination Party Address	The IP address of the called participant. A string of up to 255 characters.
Endpoint Type	The endpoint type, as follows: **0** - Terminal **1** - Gateway **2** - MCU **3** - Gatekeeper **4** - Undefined

Table C-18 *Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED*

Field	Description
Participant Name	The name of the participant. An empty field “” denotes an unidentified participant or a participant whose name is unspecified.
Participant ID	The identification number assigned to the participant by the MCU.
Participant Status	The participant status, as follows: **0** - Idle **1** - Connected **2** - Disconnected **3** - Waiting for dial-in **4** – Connecting **5** - Disconnecting **6** - Partially connected. Party has completed H.221 capability exchange **7** - Deleted by a user **8** - Secondary. The participant could not connect the video channels and is connected via audio only **10** - Connected with problem **11** - Redialing
Capabilities	Not supported. Always contains the value **0**.
Remote Communication Mode	Not supported. Always contains the value **0**.

***Table C-18** Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED (Continued)*

Field	Description
Secondary Cause	**Note:** This field is only relevant if the Participant Status is Secondary. The cause for the secondary connection (not being able to connect the video channels), as follows: **0** - Default **11** - The incoming video parameters are not compatible with the conference video parameters **13** - The conference video settings are not compatible with the endpoint capabilities **14** - The new conference settings are not compatible with the endpoint capabilities **15** - Video stream violation due to incompatible annexes or other discrepancy **16** - Inadequate video resources **17** - When moved to a Transcoding or Video Switching conference, the participant's video capabilities are not supported by the video cards **18** - Video connection could not be established **24** - The endpoint closed its video channels **25** - The participant video settings are not compatible with the conference protocol **26** - The endpoint could not re-open the video channel after the conference video mode was changed **27** - The gatekeeper approved a lower bandwidth than requested **28** - Video connection for the SIP participant is temporarily unavailable **255** - Other

***Table C-19** Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Dialing Direction	The dialing direction, as follows **0** - Dial-out **5** - Dial-in
Bonding Mode	Not supported. Always contains the value **0**.
Number of Channels	**Note:** This field is only relevant to ISDN/PSTN participants. The number of channels being connected for this participant.
Net Channel Width	Not supported. Always contains the value **0**.
Network Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.

Table C-19 *Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT (Continued)*

Field	Description
Restrict	Not supported. Always contains the value **0**.
Audio Only	Indicates the participant's Audio Only setting, as follows: **0** - The participant is *not* an Audio Only participant **1** - The participant is an Audio Only participant **255** - Unknown
Default Number Type	**Note:** This field is only relevant to ISDN/PSTN participants. The type of telephone number. **Note:** Since undefined participants are always dial-in participants, the only possible value is: **255** - Taken from Network Service
Net Sub-Service Name	Not supported. This field remains empty.
Number of Participant Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The number of participant phone numbers. The participant phone number is the CLI (Calling Line Identification) as identified by the MCU.
Number of MCU Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The number of MCU phone numbers. The MCU phone number is the number dialed by the participant to connect to the MCU.
Party and MCU Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. No, one or more fields, one field for each participant and MCU phone number. The participant phone numbers are listed first, followed by the MCU phone numbers.
Identification Method	**Note:** This field is only relevant to dial-in participants. The method by which the destination conference is identified, as follows: **1** - Called phone number, IP address or alias **2** - Calling phone number, IP address or alias
Meet Me Method	**Note:** This field is only relevant to dial-in participants. The meet-me per method, as follows: **3** - Meet-me per participant
Network Type	The type of network between the participant and the MCU, as follows: **0** - ISDN/PSTN **2** - H.323 **5** - SIP
H.243 Password	Not supported. This field remains empty.

Table C-19 *Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT (Continued)*

Field	Description
Chair	Not supported. Always contains the value **0**.
Video Protocol	The video protocol, as follows: **1** - H.261 **2** - H.263 **4** - H.264 **255** - Auto
Broadcasting Volume	The broadcasting volume assigned to the participant. The value is between **1** (lowest) and **10** (loudest). Each unit movement increases or decreases the volume by **3 dB**.
Undefined Participant	Indicates whether are not the participant is an undefined participant, as follows: **0** - The participant is *not* an undefined participant. **2** - The participant is an undefined participant.
Node Type	The node type, as follows: **0** - MCU **1** - Terminal
Bonding Phone Number	**Note:** This field is only relevant to ISDN/PSTN participants. The phone number for Bonding dial-out calls. Bonding is a communication protocol that aggregates from two up to thirty 64 Kbps B channels together, to look like one large bandwidth channel.
Video Bit Rate	The video bit rate in units of kilobits per second. A value of **4294967295** denotes auto, and in this case, the rate is computed by the MCU.
IP Address	**Note:** This field is only relevant to IP participants. The IP address of the participant. An address of **4294967295** indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Signaling Port	**Note:** This field is only relevant to IP participants. The signaling port used for participant connection. A value of **65535** is ignored by MCU.

Table C-19 *Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT (Continued)*

Field	Description
H.323 Participant Alias Type/SIP Participant Address Type	**Note:** This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: **7** - E164 **8** - H.323 ID **13** - Email ID **14** - Participant number For SIP participants, the address type, as follows: **1** - SIP URI **2** - Tel URL
H.323 Participant Alias Name/SIP Participant Address	**Note:** This field is only relevant to IP participants. For H.323 participants: The participant alias. The alias may contain up to 512 characters. For SIP participants: The participant address. The address may contain up to 80 characters.

Table C-20 *Event Fields for Event 1001 - NEW UNDEFINED PARTY CONTINUE 1*

Field	Description
Encryption	Indicates the participant's encryption setting as follows: **0** - The participant is *not* encrypted. **1** - The participant is encrypted. **2** - Auto. The conference encryption setting is applied to the participant.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Table C-21 *Event Fields for Event 20 - BILLING CODE*

Field	Description
Participant Name	The name of the participant who added the billing code.
Participant ID	The identification number, as assigned by the MCU, of the participant who added the billing code.
Billing Info	The numeric billing code that was added (32 characters).

Table C-22 *Event Fields for Event 21 - SET PARTICIPANT DISPLAY NAME*

Field	Description
Participant Name	The original name of the participant, for example, the name automatically assigned to an undefined participant, such as, “<conference name>_(000)”.
Participant ID	The identification number assigned to the participant by the MCU.
Display Name	The new name assigned to the participant by the user, or the name sent by the end point.

Table C-23 *Event Fields for Event 22 - DTMF CODE FAILURE*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Incorrect Data	The incorrect DTMF code entered by the participant, or an empty field “” if the participant did not press any key.
Correct Data	The correct DTMF code, if known.
Failure Type	The type of DTMF failure, as follows: **2** - The participant did not enter the correct conference password. **6** - The participant did not enter the correct chairperson password. **12** - The participant did not enter the correct Conference ID.

Table C-24 *Event fields for Event 26 - RECORDING LINK*

Field	Description
Participant Name	The name of the Recording Link participant.
Participant ID	The identification number assigned to the Recording Link participant by the MCU.
Recording Operation	The type of recording operation, as follows: **0** - Start recording **1** - Stop recording **2** - Pause recording **3** - Resume recording **4** - Recording ended **5** - Recording failed
Initiator	Not supported.

Table C-24 *Event fields for Event 26 - RECORDING LINK (Continued)*

Field	Description
Recording Link Name	The name of the Recording Link.
Recording Link ID	The Recording Link ID.
Start Recording Policy	The start recording policy, as follows: **1** - Start recording automatically as soon as the first participant connects to the conference. **2** - Start recording when requested by the conference chairperson via DTMF codes or from the *MCU Web Client*, or when the operator starts recording from the *MCU Web Client*.

Table C-25 *Event Fields for Event 28 - SIP PRIVATE EXTENSIONS*

Field	Description
Participant Name	The name of the participant.
Participant ID	The participant's identification number as assigned by the system.
Called Participant ID	The called participant ID.
Asserted Identity	The identity of the user sending a SIP message as it was verified by authentication.
Charging Vector	A collection of charging information.
Preferred Identity	The identity the user sending the SIP message wishes to be used for the P-Asserted-Header field that the trusted element will insert.

Table C-26 *Event Fields for Event 30 - GATEKEEPER INFORMATION*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Gatekeeper Caller ID	The caller ID in the gatekeeper records. This value makes it possible to match the CDR in the gatekeeper and in the MCU.

Table C-27 *Event fields for Event 31 - PARTICIPANT CONNECTION RATE*

Field	Description
Participant Name	The participant name.
Participant ID	The identification number assigned to the participant by the MCU.

***Table C-27** Event fields for Event 31 - PARTICIPANT CONNECTION RATE (Continued)*

Field	Description
Participant Current Rate	The participant line rate in Kbps.

***Table C-28** Event Fields for Event 32*

Field	Description
IP V6	IPv6 address of the participant's endpoint.

***Table C-29** Event fields for Event 33 - PARTY CHAIR UPDATE*

Field	Description
Participant Name	The participant name.
Participant ID	The identification number assigned to the participant by the MCU.
Chairperson	Possible values: • True - participant is a chairperson • False - Participant is not a chairperson participant (is a standard participant)

***Table C-30** Event fields for Event 34 - PARTICIPANT MAXIMUM USAGE INFORMATION*

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Maximum Bit Rate	The maximum bit rate used by the participant during the call.
Maximum Resolution	The maximum resolution used by the participant during the call. **Note:** The reported resolutions are: CIF, SD, HD720, and HD1080. Other resolutions are roundED up to the nearest resolution. For example, 2SIF is reported as SD resolution.
Maximum Frame Rate	The maximum frame rate used by the participant during the call.
Participant Address	**Note:** This field is only relevant to IP participants. For H.323 participants, the participant alias. The alias may contain up to 512 characters. For SIP participants, the participant address. The address may contain up to 80 characters.

***Table C-31** Event Fields for Event 35 - SVC SIP PARTICIPANT CONNECTED*

Field	Description
Participant Name	The name of the participant. An empty field "" denotes an unidentified participant or a participant whose name is unspecified
Participant ID	The identification number assigned to the participant by the MCU.
Participant Status	The participant status, as follows: 0 - Idle 1 - Connected 2 - Disconnected 3 - Waiting for dial-in 4 - Connecting 5 - Disconnecting 6 - Partially connected. Party has completed H.221 capability exchange 7 - Deleted by a user 8 - Secondary. The participant could not connect the video channels and is connected via audio only 10 - Connected with problem 11 - Redialing
Receive line rate	Negotiated reception line rate
Transmit line rate	Negotiated transmission line rate
Uplink Video Capabilities	a.Number of uplink streams b.Video stream (multiple streams) i.Resolution width ii.resolution height iii.max frame rate iv.max line rate
Audio Codec	SAC, Other
Secondary Cause	

***Table C-32** Event Fields for Event 100 - USER TERMINATE CONFERENCE*

Field	Description
Terminated By	The login name of the user who terminated the conference.

Table C-33 *Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT*

Field	Description
User Name	The login name of the user who reconnected the participant to the conference, or disconnected or deleted the participant from the conference.
Participant Name	The name of the participant reconnected to the conference, or disconnected or deleted from the conference.
Participant ID	The identification number assigned to the participant by the MCU.

Table C-34 *Event Fields for Event 106 - USER SET END TIME*

Field	Description
New End Time	The new conference end time set by the user, in GMT time.
User Name	The login name of the user who changed the conference end time.

Table C-35 *Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY*

Field	Description
Operator Name	The login name of the user who moved the participant.
Party Name	The name of the participant who was moved.
Party ID	The identification number of the participant who was moved, as assigned by the MCU.
Destination Conf Name	The name of the conference to which the participant was moved.
Destination Conf ID	The identification number of the conference to which the participant was moved.

Table C-36 *Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE*

Field	Description
Operator Name	The login name of the operator who moved the participant to the conference.
Source Conf Name	The name of the source conference.
Source Conf ID	The identification number of the source conference, as assigned by the MCU.
Party Name	The name of the participant who was moved.

Table C-36 Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE (Continued)

Field	Description
Party ID	The identification number assigned to the participant by the MCU.
Connection Type	The connection type, as follows: **0** - Dial-out **5** - Dial-in
Bonding Mode	**Note:** This field is only relevant to ISDN/PSTN participants. Possible values are: **0** - Bonding is disabled **1** - Bonding is enabled **255** - Auto
Number Of Channels	**Note:** This field is only relevant to ISDN/PSTN participants. The number of channels, as follows: **255** - Auto Otherwise, in range of **1** - **30**
Net Channel Width	The bandwidth of each channel. This value is always **0**, which represents a bandwidth of **1B**, which is the only bandwidth that is currently supported.
Net Service Name	The name of the Network Service. An empty field “” indicates the default Network Service.
Restrict	Indicates whether or not the line is restricted, as follows: **27** - Restricted line **28** - Non restricted line **255** - Unknown or not relevant
Voice Mode	Indicates whether or not the participant is an Audio Only participant, as follows: **0** - The participant is *not* an Audio Only participant **1** - The participant is an Audio Only participant **255** - Unknown
Number Type	**Note:** This field is only relevant to dial-out, ISDN/PSTN participants. The type of telephone number, as follows: **0** - Unknown **1** - International **2** - National **3** - Network specific **4** - Subscriber **6** - Abbreviated **255** - Taken from Network Service, default

Table C-36 *Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE (Continued)*

Field	Description
Net SubService Name	**Note:** This field is only relevant to dial-out, ISDN/PSTN participants. The network sub-service name. An empty field "" means that MCU selects the default sub-service.
Number of Party Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The number of participant phone numbers. In a dial-in connection, the participant phone number is the CLI (Calling Line Identification) as identified by the MCU. In a dial-out connection, participant phone numbers are the phone numbers dialed by the MCU for each participant channel.
Number of MCU Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The number of MCU phone numbers. In a dial-in connection, the MCU phone number is the number dialed by the participant to connect to the MCU. In a dial-out connection, the MCU phone number is the MCU (CLI) number as seen by the participant.
Party and MCU Phone Numbers	**Note:** This field is only relevant to ISDN/PSTN participants. The participant phone numbers are listed first, followed by the MCU phone numbers.
Ident. Method	**Note:** This field is only relevant to dial-in participants. The method by which the destination conference is identified, as follows: **0** - Password **1** - Called phone number, or IP address, or alias **2** - Calling phone number, or IP address, or alias
Meet Method	**Note:** This field is only relevant to dial-in participants. The meet-me per method, as follows: **1** - Meet-me per MCU-Conference **3** - Meet-me per participant **4** - Meet-me per channel
Net Interface Type	The type of network interface between the participant and the MCU, as follows: **0** - ISDN **2** - H.323 **5** - SIP
H243 Password	The H.243 password, or an empty field "" if there is no password.
Chair	Not supported. Always contains the value **0**.

Table C-36 *Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE (Continued)*

Field	Description
Video Protocol	The video protocol, as follows: **1** - H.261 **2** - H.263 **3** - H.264* **4** - H.264 **255** - Auto
Audio Volume	The broadcasting volume assigned to the participant. The value is between **1** (lowest) and **10** (loudest).
Undefined Type	The participant type, as follows: **0** - Defined participant. (The value in the formatted text file is “default”.) **2** - Undefined participant. (The value in the formatted text file is “Unreserved participant “.)
Node Type	The node type, as follows: **0** - MCU **1** - Terminal
Bonding Phone Number	**Note:** This field is only relevant to ISDN/PSTN participants. The phone number for Bonding dial-out calls.
Video Rate	**Note:** This field is only relevant to IP participants. The video rate in units of kilobits per second. A value of **4294967295** denotes auto, and in this case, the rate is computed by the MCU.
IP Address	**Note:** This field is only relevant to IP participants. The IP address of the participant. An address of **4294967295** indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Call Signaling Port	**Note:** This field is only relevant to IP participants. The signaling port used for participant connection. A value of **65535** is ignored by MCU.

***Table C-36** Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE (Continued)*

Field	Description
H.323 Party Alias Type/SIP Party Address Type	**Note:** This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: **7** - E164 **8** - H.323 ID **11** - URL ID alias type **12** - Transport ID **13** - Email ID **14** - Participant number For SIP participants, the address type, as follows: **1** - SIP URI **2** - Tel URL
H.323 Party Alias/ SIP Party Address	**Note:** This field is only relevant to IP participants. For H.323 participants, the participant alias. The alias may contain up to 512 characters. For SIP participants, the participant address. The address may contain up to 80 characters.

***Table C-37** Event Fields for Event 111 - OPERATOR BACK TO CONFERENCE PARTY*

Field	Description
Operator Name	The login name of the operator moving the participant back to the conference.
Party Name	The name of the participant being moved.
Party ID	The identification number, as assigned by the MCU, of the participant being moved.

***Table C-38** Event Fields for Events 2011, 2012, and 2016*

Field	Description
IP V6	IPv6 address of the participant’s endpoint.

Table C-39 *Event Fields for Event 3010 - PARTICIPANT INFORMATION*

Field	Description
Info1 *Info2* *Info3* *Info4*	The participant information fields. These fields enable users to enter general information about the participant, such as the participant's e-mail address. The maximum length of each field is 80 characters.
VIP	Not supported. Always contains the value **0**.

Disconnection Cause Values

For an explanation of the disconnection causes, see *Appendix A: "Disconnection Causes"* on page **A-1**.

Table C-40 *Disconnection Cause Values*

Value	Call Disconnection Cause
0	Unknown
1	Participant hung up
2	Disconnected by User
5	Resources deficiency
6	Password failure
20	H323 call close. No port left for audio
21	H323 call close. No port left for video
22	H323 call close. No port left for FECC
23	H323 call close. No control port left
25	H323 call close. No port left for video content
51	A common key exchange algorithm could not be established between the MCU and the remote device
53	Remote device did not open the encryption signaling channel
59	The remote devices' selected encryption algorithm does not match the local selected encryption algorithm
141	Called party not registered
145	Caller not registered
152	H323 call close. ARQ timeout

Table C-40 Disconnection Cause Values (Continued)

Value	Call Disconnection Cause
153	H323 call close. DRQ timeout
154	H323 call close. Alt Gatekeeper failure
191	H323 call close. Remote busy
192	H323 call close. Normal
193	H323 call close. Remote reject
194	H323 call close. Remote unreachable
195	H323 call close. Unknown reason
198	H323 call close. Small bandwidth
199	H323 call close. Gatekeeper failure
200	H323 call close. Gatekeeper reject ARQ
201	H323 call close. No port left
202	H323 call close. Gatekeeper DRQ
203	H323 call close. No destination IP value
204	H323 call close. Remote has not sent capability
205	H323 call close. Audio channels not open
207	H323 call close. Bad remote cap
208	H323 call close. Capabilities not accepted by remote
209	H323 failure
210	H323 call close. Remote stop responding
213	H323 call close. Master slave problem
251	SIP timer popped out
252	SIP card rejected channels
253	SIP capabilities don't match
254	SIP remote closed call
255	SIP remote cancelled call
256	SIP bad status
257	SIP remote stopped responding
258	SIP remote unreachable
259	SIP transport error
260	SIP bad name

Table C-40 Disconnection Cause Values (Continued)

Value	Call Disconnection Cause
261	SIP trans error TCP invite
300	SIP redirection 300
301	SIP moved permanently
302	SIP moved temporarily
305	SIP redirection 305
380	SIP redirection 380
400	SIP client error 400
401	SIP unauthorized
402	SIP client error 402
403	SIP forbidden
404	SIP not found
405	SIP client error 405
406	SIP client error 406
407	SIP client error 407
408	SIP request timeout
409	SIP client error 409
410	SIP gone
411	SIP client error 411
413	SIP client error 413
414	SIP client error 414
415	SIP unsupported media type
420	SIP client error 420
480	SIP temporarily not available
481	SIP client error 481
482	SIP client error 482
483	SIP client error 483
484	SIP client error 484
485	SIP client error 485
486	SIP busy here
487	SIP request terminated
488	SIP client error 488

***Table C-40** Disconnection Cause Values (Continued)*

Value	Call Disconnection Cause
500	SIP server error 500
501	SIP server error 501
502	SIP server error 502
503	SIP server error 503
504	SIP server error 504
505	SIP server error 505
600	SIP busy everywhere
603	SIP global failure 603
604	SIP global failure 604
606	SIP global failure 606

MGC Manager Events that are not Supported by the MCU

The following MGC Manager events are not supported by the MCU:

For details of these events see the M*GC Manager User's Guide Volume II*, *Appendix A*.

- Event 8 - REMOTE COM MODE
- Event 11 - ATM CHANNEL CONNECTED
- Event 12 - ATM CHANNEL DISCONNECTED
- Event 13 - MPI CHANNEL CONNECTED
- Event 14 - MPI CHANNEL DISCONNECTED
- Event 15 - H323 CALL SETUP
- Event 16 - H323 CLEAR INDICATION
- Event 24 - SIP CALL SETUP
- Event 25 - SIP CLEAR INDICATION
- Event 27 - RECORDING SYSTEM LINK
- Event 110 - OPERATOR ON HOLD PARTY
- Event 113 - CONFERENCE REMARKS
- Event 2108 - OPERATOR MOVE PARTY TO CONFERENCE CONTINUE 1
- Event 3001 - CONFERENCE START CONTINUE 2
- Event 3108 - OPERATOR MOVE PARTY TO CONFERENCE CONTINUE 2
- Event 4001 - CONFERENCE START CONTINUE 3
- Event 4108 - OPERATOR MOVE PARTY TO CONFERENCE CONTINUE 3

Appendix D

Ad Hoc Conferencing and External Database Authentication

The RealPresence Collaboration Server (RMX) Ad Hoc conferencing feature enables participants to start ongoing conferences on-the-fly, without prior definition when dialing an Ad Hoc-enabled Entry Queue. The created conference parameters are taken from the Profile assigned to the Ad Hoc-enabled Entry Queue.

Ad Hoc conferencing is available in two modes:

- Ad Hoc Conferencing without Authentication

  Any participant can dial into an Entry Queue and initiate a new conference if the conference does not exist. This mode is usually used for the organization's internal Ad Hoc conferencing.
- **Ad Hoc Conferencing with External Database Authentication**

  In this mode, the participant's right to start a new conference is validated against a database.

The external database application can also be used to validate the participant's right to join an ongoing conference. Conference access authentication can be:

- Part of the Ad Hoc conferencing flow where the participants must be authorized before they can enter the conference created in the Ad Hoc flow.
- Independent of Ad Hoc conferencing where conference access is validated for all conferences running on the MCU regardless of the method in which the conference was started.

Ad Hoc Conferencing without Authentication

A participant dials in to an Ad Hoc-enabled Entry Queue and starts a new conference based on the Profile assigned to the Entry Queue. In this configuration, any participant connecting to the Entry Queue can start a new conference, and no security mechanism is applied. This mode is usually used in organizations where Ad Hoc conferences are started from within the network and without security breach.

Starting a conference uses the following method:

1. The participant dials in to the Ad Hoc-enabled Entry Queue.
2. The Conference ID is requested by the system.
3. The participant inputs a Conference ID via his/her endpoint remote control using DTMF codes.

4 The MCU checks whether a conference with the same Conference ID is running on the MCU. If there is such a conference, the participant is moved to that conference. If there is no ongoing conference with that Conference ID, the system creates a new conference, based on the Profile assigned to the Entry Queue, and connects this participant as the conference chairperson.

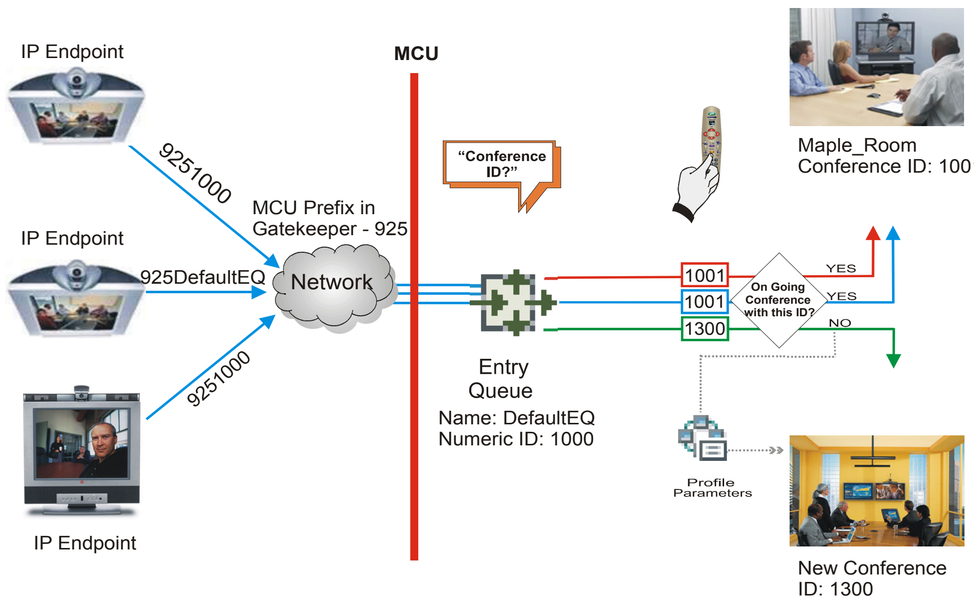


Figure D-1 *Ad Hoc Conference Initiation without Authentication*

To enable this workflow, the following components must be defined in the system:

- An Entry Queue IVR Service with the appropriate audio file requesting the Conference ID
- An Ad Hoc-enabled Entry Queue with an assigned Profile

Ad Hoc Conferencing with Authentication

The MCU can work with an external database application to validate the participant's right to start a new conference. The external database contains a list of participants, with their assigned parameters. The conference ID entered by the participant is compared against the database. If the system finds a match, the participant is granted the permission to start a new conference.

To work with an external database application to validate the participant's right to start a new conference, the Entry Queue IVR Service must be configured to use the external database application for authentication. In the external database application, you must define all participants (users) with rights to start a new conference using Ad Hoc conferencing. For each user defined in the database, you enter the conference ID, Conference Password (optional) and Chairperson Password (when applicable), billing code, Conference general information (corresponding to the User Defined 1 field in the Profile properties) and user's PIN code. The same user definitions can be used for conference access authentication, that is, to determine who can join the conference as a participant and who as a chairperson.

Entry Queue Level - Conference Initiation Validation with an External Database Application

Starting a new conference with external database application validation entails the following steps:

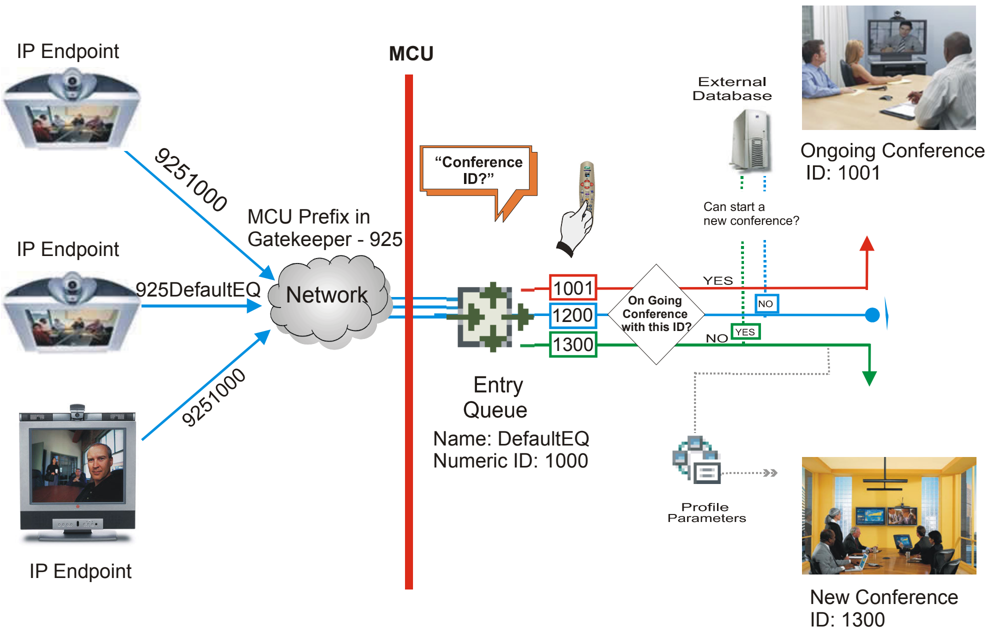


***Figure D-2** Conference Initiation Validation with External Database Application*

1 The participant dials in to an Ad Hoc-enabled Entry Queue.

2 The participant is requested to enter the Conference ID.

3 The participant enters the conference ID via his/her endpoint remote control using DTMF codes. If there is an ongoing conference with this Conference ID, the participant is moved to that conference where another authentication process can occur, depending on the IVR Service configuration.

4 If there is no ongoing conference with that Conference ID, the MCU verifies the Conference ID with the database application that compares it against its database. If the database application finds a match, the external database application sends a response back to the MCU, granting the participant the right to start a new ongoing conference.

If this Conference ID is not registered in the database, the conference cannot be started and this participant is disconnected from the Entry Queue.

5 The external database contains a list of participants (users), with their assigned parameters. Once a participant is identified in the database (according to the conference ID), his/her parameters (as defined in the database) can be sent to the MCU in the same response granting the participant the right to start a new ongoing conference. These parameters are:

— Conference Name

— Conference Billing code

— Conference Password

— Chairperson Password

— Conference Information, such as the contact person name. These fields correspond to Info 1, 2 and 3 fields in the *Conference Properties - Information* dialog box.
— Maximum number of participants allowed for the conference
— Conference Owner

These parameters can also be defined in the conference Profile. In such a case, parameters sent from the database overwrite the parameters defined in the Profile. If these parameters are not sent from the external database to the MCU, they will be taken from the Profile.

6. A new conference is started based on the Profile assigned to the Entry Queue.
7. The participant is moved to the conference.
If no password request is configured in the Conference IVR Service assigned to the conference, the participant that initiated the conference is directly connected to the conference, as its chairperson.

   If the Conference IVR Service assigned to the conference is configured to prompt for the conference password and chairperson password, without external database authentication, the participant has to enter these passwords in order to join the conference.

To enable this workflow, the following components must be defined in the system:

- A Conference IVR Service with the appropriate prompts. If conference access is also validated with the external database application it must be configured to access the external database for authentication.
- An Entry Queue IVR Service configured with the appropriate audio prompts requesting the Conference ID and configured to access the external database for authentication.
- Create a Profile with the appropriate conference parameters and the appropriate Conference IVR Service assigned to it.
- An Ad Hoc-enabled Entry Queue with the appropriate Entry Queue IVR Service and Conference Profile assigned to it.
- An external database application with a database containing Conference IDs associated with participants and their relevant properties.
- Define the flags required to access the external database in System Configuration.

  For more information, see Figure , "*MCU Configuration to Communicate with an External Database Application*" on page **D-9**.

Conference Access with External Database Authentication

The MCU can work with an external database application to validate the participant's right to join an existing conference. The external database contains a list of participants, with their assigned parameters. The conference password or chairperson password entered by the participant is compared against the database. If the system finds a match, the participant is granted the permission to access the conference.

To work with an external database application to validate the participant's right to join the conference, the Conference IVR Service must be configured to use the external database application for authentication.

Conference access authentication can be performed as:

- Part of the Ad Hoc conferencing flow where the participants must be authorized before they can enter the conference created in the Ad Hoc flow
- Independent of Ad Hoc conferencing where conference access is validated for all conferences running on the MCU regardless of the method in which the conference was started.

Conference access authentication can be implemented for all participants joining the conference or for chairpersons only.

Conference Access Validation - All Participants (Always)

Once the conference is created either via an Ad Hoc Entry Queue, or a standard ongoing conference, the right to join the conference is authenticated with the external database application for all participants connecting to the conference.

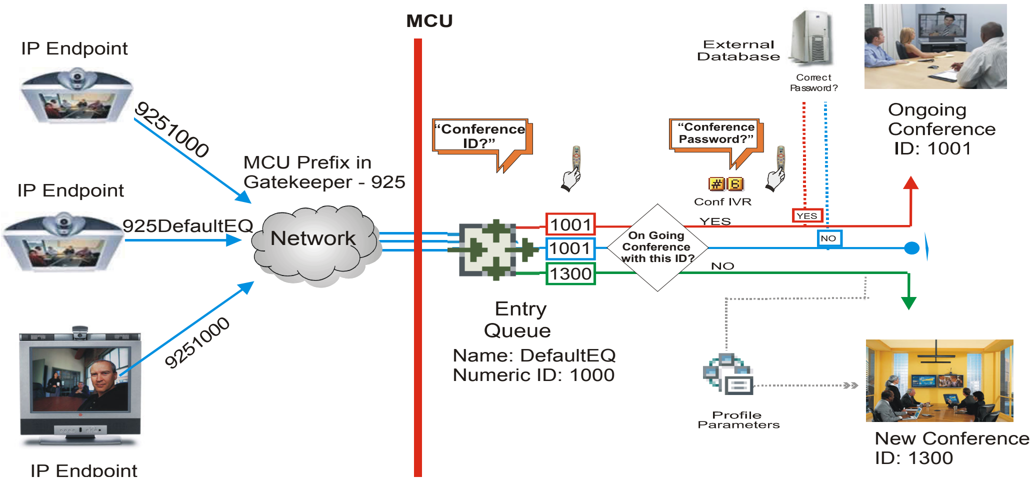


Figure D-3 *Conference Access - Conference Password validation with External Database Application*

Joining the conference entails the following steps:

- When the conference is started (either in the Ad Hoc flow or in the standard method), all participants connecting to the conference are moved to the Conference IVR queue where they are prompted for the conference password.
- When the participant enters the conference password or his/her personal password, it is sent to the external database application for validation.
- If there is a match, the participant is granted the right to join the conference. In addition, the external database application sends to the MCU the following parameters:
  - — Participant name (display name)
  - — Whether or not the participant is the conference chairperson
  - — Participant Information, such as the participant E-mail. These fields correspond to Info 1, 2, 3 and 4 fields in the *Participant Properties - Information* dialog box.

  If there is no match (i.e. the conference or personal password are not defined in the database), the request to access the conference is rejected and the participant is disconnected from the MCU.

- If the Conference IVR Service is configured to prompt for the chairperson identifier and password, the participant is requested to enter the chairperson identifier.
  — If no identifier is entered, the participant connects as a standard, undefined participant.
- If the chairperson identifier is entered, the participant is requested to enter the chairperson password. In this flow, the chairperson password is **not** validated with the external database application, only with the MCU.
  — If the correct chairperson password is entered, the participant is connected to the conference as its chairperson.
  — If the wrong password is entered, he/she is disconnected from the conference.

To enable conference access validation for all participants the following conferencing components are required:

- The external database must hold the conference password or the participant personal password/PIN code or the participant's Alias.
- The Conference IVR Service assigned to the conference (defined in the Profile) must be configured to authenticate the participant's right to access the conference with the external database application for all requests. In addition it must be configured to prompt for the Conference Password.

Conference Access Validation - Chairperson Only (Upon Request)

An alternative validation method at the conference level is checking only the chairperson password with the external database application. All other participants can be checked only with the MCU (if the Conference IVR Service is configured to prompt for the conference password) or not checked at all (if the Conference IVR Service is configured to prompt only for the chairperson password).

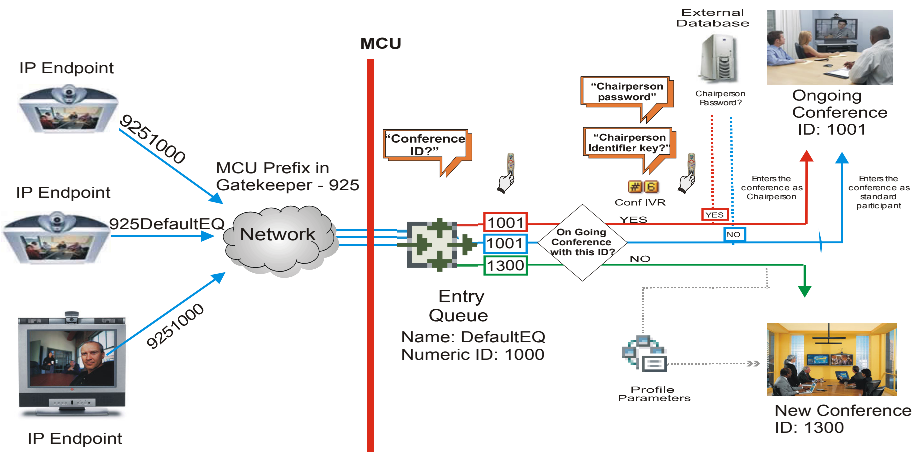


Figure D-4 Conference Access - Chairperson Password validation with external database application

Joining the conference entails the following steps:

- When the conference is started (either in the Ad Hoc flow or in the standard method), all participants connecting to the conference are moved to the conference IVR queue where they are prompted for the conference password.

- If the Conference IVR Service is configured to prompt for the Conference password, the participant is requested to enter the conference password. In this flow, the conference password is **not** validated with the external database application, only with the MCU.
  — If the wrong password is entered, he/she is disconnected from the conference.
- If the correct conference password is entered, the participant is prompted to enter the chairperson identifier key.
  — If no identifier is entered, the participant is connected to the conference as a standard participant.
- If the chairperson identifier is entered, the participant is prompted to enter the chairperson password.
- When the participant enters the chairperson password or his/her personal password, it is sent to the external database application for validation.
  — If the password is incorrect the participant is disconnected from the MCU.
- If there is a match, the participant is granted the right to join the conference as chairperson. In addition, the external database application sends to the MCU the following parameters:
  — Participant name (display name)
  — Participant Information, such as the participant E-mail. These fields correspond to Info 1, 2, 3 and 4 fields in the *Participant Properties - Information* dialog box.

To enable conference access validation for all participants the following conferencing components are required:

- The external database must hold the Chairperson Password or the participant's Alias.
- The Conference IVR Service assigned to the conference (defined in the Profile) must be configured to check the external database for the Chairperson password only when the participant enters the chairperson identifier key (either pound or star). In addition, it must be configured to prompt for the chairperson identifier key and password.

System Settings for Ad Hoc Conferencing and External Database Authentication

Ad Hoc Settings

Before a participant can initiate an Ad Hoc conference (with or without authentication), the following components must be defined:

- **Profiles**

  Defines the conference parameters for the conferences that will be initiated from the Ad Hoc-enabled Entry Queue. For more details, see "*Conference Profiles"* on page **2-1**.
- **Entry Queue IVR Service with Conference ID Request Enabled**

  The Entry Queue Service is used to route participants to their destination conferences, or create a new conference with this ID. For details, see "*IVR Services"* on page **17-1**.

  In Ad Hoc conferencing, the Conference ID is used to check whether the destination conference is already running on the MCU and if not, to start a new conference using this ID.

- **Ad Hoc - enabled Entry Queue**

  Ad Hoc conferencing must be enabled in the Entry Queue and a Profile must be assigned to the Entry Queue. In addition, an Entry Queue IVR Service supporting conference ID request. For details, see "*Entry Queues"* on page **7-1**.

Authentication Settings

- **MCU Configuration**

  Usage of an external database application for authentication (for starting new conferences or joining ongoing conferences) is configured for the MCU in the System Configuration. For details, see "*MCU Configuration to Communicate with an External Database Application"* on page **D-9**.
- **Entry Queue IVR Service with Conference Initiation Authentication Enabled**

  Set the Entry Queue IVR Service to send authentication requests to the external database application to verify the participant's right to start a new conference according to the Conference ID entered by the participant. For details, see "*Enabling External Database Validation for Starting New Ongoing Conferences"* on page **D-10**.
- **Conference IVR Service with Conference Access Authentication Enabled**

  Set the Conference IVR Service to send authentication requests to the external database application to verify the participant's right to connect to the conference as a standard participant or as a chairperson. For details, see "*Enabling External Database Validation for Conferences Access"* on page **D-10**.
- **External Database Application Settings**

  The external database contains a list of participants (users), with their assigned parameters. These parameters are:

  — Conference Name

  — Conference Billing code

  — Conference Password

  — Chairperson Password

  — Conference Information, such as the contact person name. These fields correspond to Info 1, 2 and 3 fields in the *Conference Properties - Information* dialog box.

  — Maximum number of participants allowed for the conference

  — Conference Owner

  — Participant name (display name)

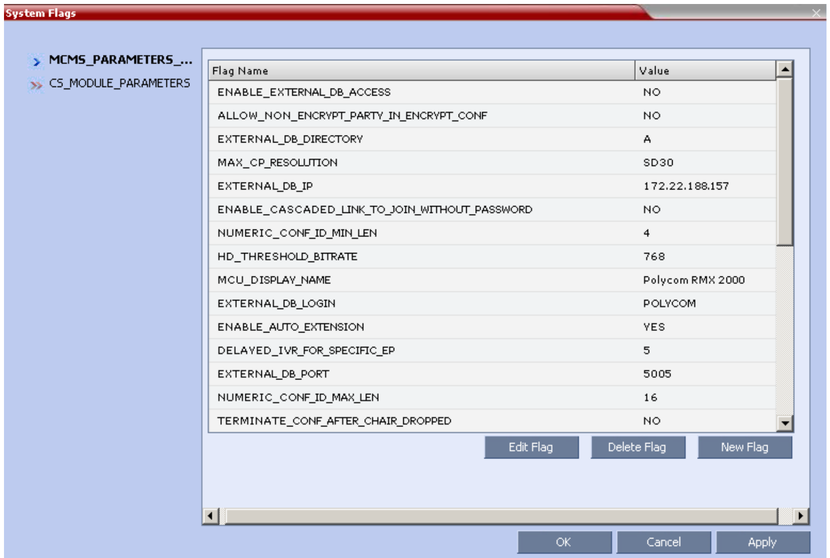
  — Participant Information, such as the participant E-mail. These fields correspond to Info 1, 2, 3 and 4 fields in the *Participant Properties - Information* dialog box.

MCU Configuration to Communicate with an External Database Application

To enable the communication with the external database application, several flags must be set in the System Configuration.

To set the System Configuration flags:

1 On the *Setup* menu, click **System Configuration**.
The *System Flags* dialog box opens.



2 Modify the values of the following flags:

Table D-1 *Flag Values for Accessing External Database Application*

Flag	Description and Value
ENABLE_EXTERNAL_DB_ACCESS	The flag that enables the use of the external database application.
EXTERNAL_DB_IP	The IP address of the external database application server. default IP: 0.0.0.0.
EXTERNAL_DB_PORT	The port number used by the MCU to access the external application server. Default Port = 80.
EXTERNAL_DB_LOGIN	The user name defined in the external database application for the MCU.
EXTERNAL_DB_PASSWORD	The password associated with the user name defined for the MCU in the external database application.
EXTERNAL_DB_DIRECTORY	The URL of the external database application.

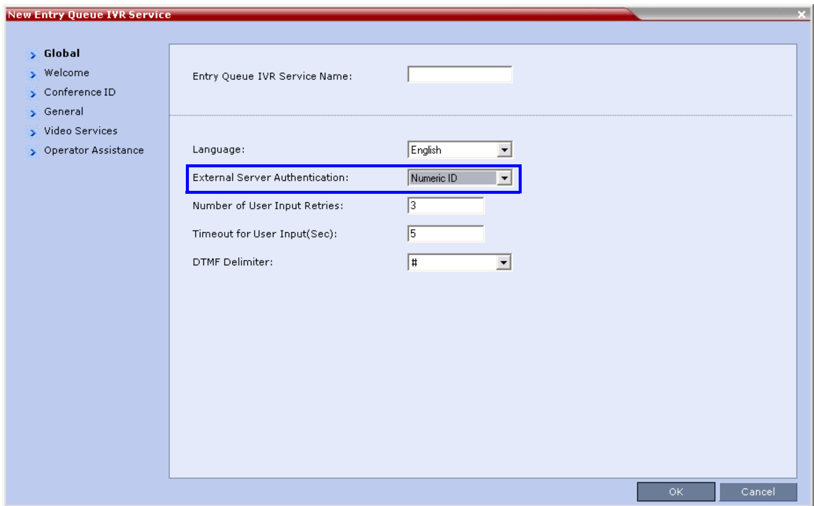
3 Click **OK**.

4 Reset the MCU for flag changes to take effect.

Enabling External Database Validation for Starting New Ongoing Conferences

The validation of the participant's right to start a new conference with an external database application is configured in the *Entry Queue IVR Service - Global* dialog box.

>> Set the *External Server Authentication* field to **Numeric ID**.



Enabling External Database Validation for Conferences Access

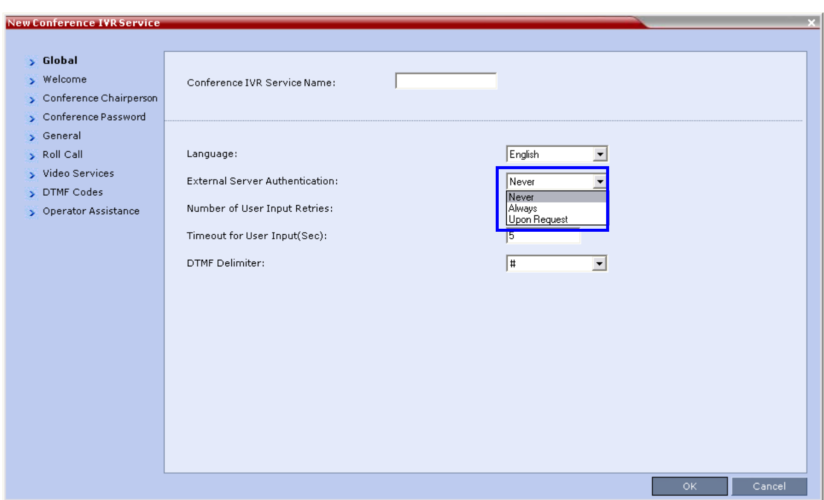
The validation of the participant's right to join an ongoing conference with an external database application is configured in the *Conference IVR Service - Global* dialog box.

You can set the system to validate all the participants joining the conference or just the chairperson.

>> Set the *External Server Authentication* field to:

— **Always -** to validate the participant's right to join an ongoing conference for all participants

— **Upon Request** - to validate the participant's right to join an ongoing conference as chairperson



Appendix E

Participant Properties Advanced Channel Information

The following appendix details the properties connected with information about audio and video parameters, as well as, problems with the network which can affect the audio and video quality.

Table E-1 *Participant Properties - Channel Status Advanced Parameters*

Field	Description
Media Info	
Algorithm	Indicates the audio or video algorithm and protocol.
Frame per packet (audio only)	The number of audio frames per packet that are transferred between the MCU and the endpoint. If the actual Frame per Packets are higher than Frame per Packets declared during the capabilities exchange, a Faulty flag is displayed.
Resolution (video only)	Indicates the video resolution in use. If the actual resolution is higher than resolution declared in the capabilities exchange, the Faulty flag is displayed. For example, if the declared resolution is CIF and the actual resolution is 4CIF, the Faulty flag is displayed.
Frame Rate (video only)	The number of video frames per second that are transferred between the MCU and the endpoint.
Annexes (video only)	Indicates the H.263 annexes in use at the time of the last RTCP report. If the actual annexes used are other than the declared annexes in the capabilities exchange, the Faulty flag is displayed.
Channel Index	For Polycom Internal use only.

Table E-1 *Participant Properties - Channel Status Advanced Parameters*

Field	Description
RTP Statistics	
Actual loss	The number of missing packets counted by the IP card as reported in the last RTP Statistics report. If a packet that was considered lost arrives later, it is deducted from the packet loss count. Packet loss is displayed with the following details: • ***Accumulated N*** - number of lost packets accumulated since the channel opened. • ***Accumulated %*** - percentage of lost packets out of the total number of packets transmitted since the channel opened. • ***Interval N*** - number of packets lost in the last RTP report interval (default interval is 5 minutes). • ***Interval %*** - percentage of lost packets out of the total number of packets transmitted in the last RTP report interval (default interval is 5 minutes). • ***Peak*** - the highest number of lost packets in a report interval from the beginning of the channel's life span.
Out of Order	The number of packets arriving out of order. The following details are displayed: • ***Accumulated N*** - total number of packets that arrived out of order since the channel opened. • ***Accumulated %*** - percentage of packets that arrived out of order out of the total number of packets transmitted since the channel opened. • ***Interval N*** - number of packets that arrived out of order in the last RTP report interval (default interval is 5 minutes). • ***Interval %*** - percentage of packets that arrived out of order out of the total number of packets transmitted in the last RTP report interval (default interval is 5 minutes). • ***Peak*** - the highest number of packets that arrived out of order in a report interval from the beginning of the channel's life span.

Table E-1 Participant Properties - Channel Status Advanced Parameters

Field	Description
Fragmented	Indicates the number of packets that arrived to the IP card fragmented (i.e., a single packet broken by the network into multiple packets). This value can indicate the delay and reordering of fragmented packets that require additional processing, but is not considered a fault. The Fragmented information is displayed with the following details: • ***Accumulated N*** - total number of packets that were fragmented since the channel opened. • ***Accumulated %*** - percentage of fragmented packets out of the total number of packets transmitted since the channel opened. • ***Interval N*** - number of fragmented packets received in the last RTP report interval (default interval is 5 minutes). • ***Interval %*** - percentage of fragmented packets out of the total number of packets transmitted in the last RTP report interval (default interval is 5 minutes). • ***Peak*** - the highest number of fragmented packets in a report interval from the beginning of the channel's life span.

Appendix F

Secure Communication Mode

The RealPresence Collaboration Server (RMX) can be configured to work in *Secure Mode* by configuring the MCU and the *RealPresence Collaboration Server (RMX) Web Client* to work with SSL/TLS.

In this mode, a SSL/TLS Certificate is installed on the MCU, setting the MCU Listening Port to secured port 443.

TLS is a cryptographic protocol used to ensure secure communications on public networks. TLS uses a *Certificate* purchased from a trusted third party *Certificate Authority* to authenticate public keys that are used in conjunction with private keys to ensure secure communications across the network.

The MCU supports:

- TLS 1.0
- SSL 3.0 (Secure Socket Layer)

SSL 3.0 utilizes 1024-bit RSA public key encryption.

TLS certificates can be generated using the following methods: CSR, PFX and PEM; each giving different options for *Encryption Key* length. Table F-1 lists the *SIP TLS Encryption Key* length support for the various system components.

Table F-1 *SIP TLS - Encryption Key Support by System Component*

System Component	Key Generation Method	Key Length (bits)	Key generated by
SIP Signaling	CSR	2048	MCU
	PFX / PEM	1024 or 2048	User
Management	CSR	2048	MCU
LDAP			

Certificate Configuration and Management

All *Polycom* devices used in a *Maximum Security Environment* require security certificates.

Certificate Template Requirements

The specific security certificate requirements for *RMXs* used in *Maximum Security Environments* are:

- Support of 2048-bit encryption keys.
- Support of *Extended Key Usage* (*EKU*) for both:

— *Client Authentication*
— *Server Authentication*

The certificate template used by your *CA* server may need modification to meet the *RMX* requirements.

Certificate Requirements for Polycom Devices

Each *Polycom* device must have security certificates for the entire *Chain Of Trust.*

The *RMX* must have:

- The public certificate of each server in the *CA Chain* or hierarchy that issued its certificate.
  For example: *RootCA* ↔ *IntermediateCA* ↔ *SubCA*

The public certificates of the chain that issued the administrator's identity certificate. For example: *UserRootCA* ↔ *UserIntermediateCA* ↔ *UserSubCA*

Configure Certificate Management

Within a *PKI* environment, certificate revocation policies are used to ensure that certificates are valid. Certificates can expire or be revoked for various reasons (RFC 5280).

The *RMX* enforces these certificate revocation policies through *Certificate Revocation Lists* (*CRLs*). *CRLs* are required for each *CA Chain* in use by the *RMX*. These *CRL* files must be kept current

Switching to Secure Mode

The following operations are required to switch the MCU to *Secure Mode*:

- Purchase and Install the *SSL/TLS certificate*
- Modify the *Management Network* settings
- Create/Modify the relevant *System Flags*

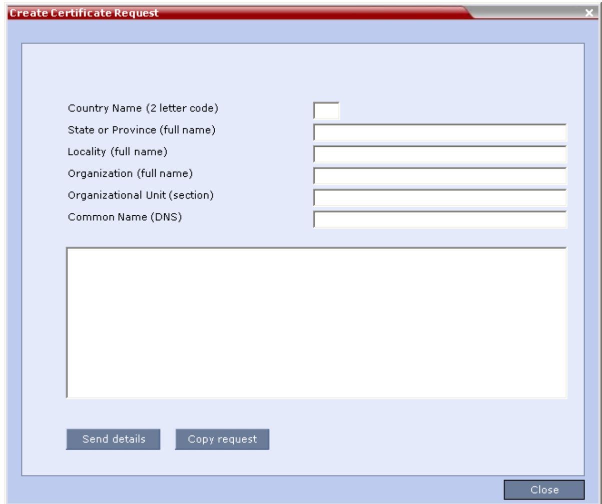
Purchasing a Certificate

Once a certificate is purchased and received it is stored in the MCU and used for all subsequent secured connections.

To create/purchase a certificate:

1 In the RMX menu, click **Setup > RMX Secured Communication > Create certificate request**.

The *Create Certificate Request* dialog box is displayed.



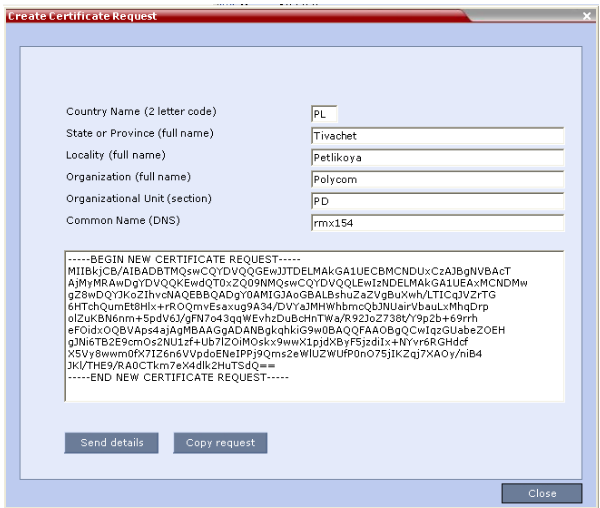
2 Enter information in all the following fields:

Table F-2 *Create Certificate Request*

Field	Description
Country Name	Enter any 2 letter code for the country name.
State or Province	Enter the full name of the state or province.
Locality	Enter the full name of the town/city/location.
Organization	Enter the full name of your organization for which the certificate will be issued.
Organizational Unit	Enter the full name of the unit (group or division) for which the certificate will be issued.
Common Name (DNS/ IP)	Enter the *DNS MCU Host Name*. This *MCU Host Name* must also be configured in the *Management Network Properties* dialog box.

3 Click **Send Details**.

The MCU creates a *New Certificate Request* and returns it to the *Create Certificate Request* dialog box along with the information the user submitted.



4 Click **Copy Request** to copy the *New Certificate Request* to the workstation's clipboard.

5 Connect to your preferred *Certificate Authority's* website using the web browser.

6 Follow the purchasing instructions at the *Certificate Authority's* website.
Paste **(Ctrl + V)** the *New Certificate Request* as required by the *Certificate Authority*.

The *Certificate Authority* issues the TLS/SSL certificate, and sends the certificate to you by e-mail.

Installing the Certificate

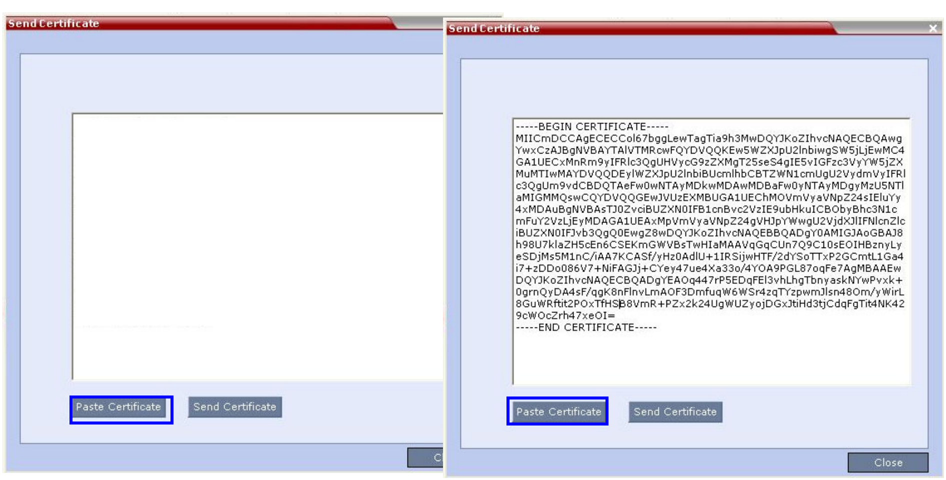
To install the certificate:

After you have received the certificate from the *Certificate Authority:*

1 **Copy** (**Ctrl + C**) the certificate information from the *Certificate Authority's* e-mail to the clipboard.

2 In the RMX menu, click **Setup > MCU Secured Communication > Send Certificate**.

3 Click **Paste Certificate** to paste the clipboard content into the *Send Certificate* dialog box.



4 Click the **Send Certificate** button to send the certificate to the MCU.

The MCU validates the certificate.

— If the certificate is not valid, an error message is displayed.

— If the certificate matches the private key, and the task is completed, a confirmation message indicating that the certificate was created successfully is displayed.

A *System Restart* is **not** required at this point.

The certificate expiry date is checked daily. An active alarm is raised two weeks before the certificate is due to expire, stating the number of days to expiry.

If the certificate expires, the MCU continues to work in secure mode and an *Active Alarm* is raised with *Security mode failed – Certificate expired* in the description field.

Certificates are deleted when an administrator performs a *Restore Factory Defaults* with the *Comprehensive Restore* option selected.

Creating/Modifying System Flags

The following *System Flags* in *system.cfg* control secure communications.

- *RMX_MANAGEMENT_SECURITY_PROTOCOL*
- *EXTERNAL_DB_PORT*

Appendix F, "System Flags" , below, lists both flags and their settings.

If the *System Flag*, *RMX_MANAGEMENT_SECURITY_PROTOCOL* does not exist in the system, it must be created by using the *RMX Setup* menu.

For more information see "*Modifying System Flags"* on page **22-1**.

Table F-3 *System Flags*

Flag	Description
RMX_MANAGEMENT_ SECURITY_PROTOCOL	Enter the protocol to be used for secure communications. Default: TLSV1_SSLV3 (both). Default for U.S. Federal licenses: TLSV1.
EXTERNAL_DB_PORT	The external database server port used by the MCU to send and receive XML requests/responses. For secure communications set the value to 443. Default: 5005.

The MCU must be restarted for modified flag settings to take effect.

Enabling Secure Communication Mode

After the SSL/TLS Certificate is installed, secure communications are enabled by modifying the properties of the *Management Network* in the *Management Network* properties dialog box.

When *Secure Communications Mode* is enabled:

- Only **`https://`** commands from the browser to the *Control Unit IP Address* of the MCU are accepted.
- The MCU listens only on secured port 443.
- All connection attempts on port 80 are rejected.

- A secure communication indicator ( ) is displayed in the browser's status bar.

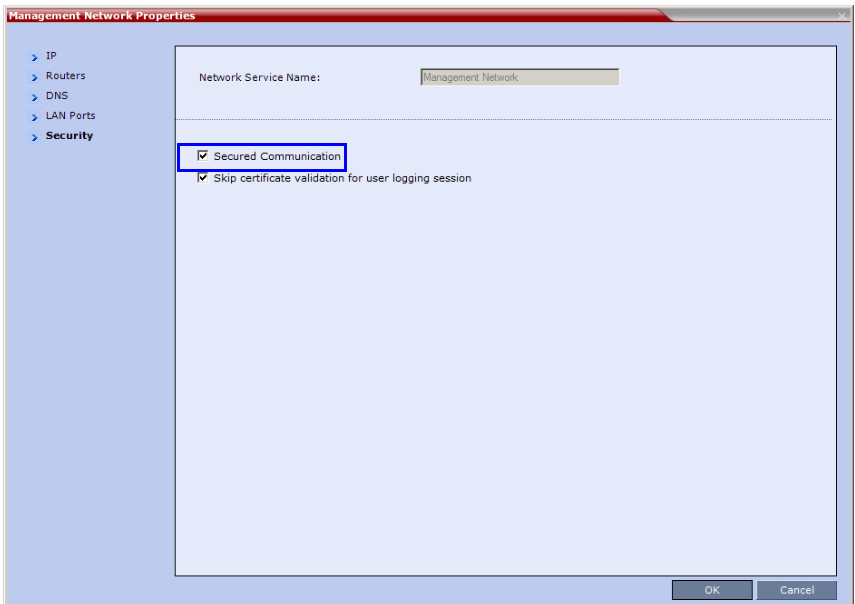
To enable secure communications mode:

1 In the *RMX Management* pane, click **IP Network Services.**

2 In the *IP Network Services* list pane, double-click the **Management Network** entry.

3 Click the **Security** tab.

The *Management Security Properties* dialog box is displayed.



4 Select the **Secured Communication** check box.

5 Click **OK**.

Alternate Management Network

The *Alternate Management Network* enables direct access to the MCU for support purposes. Access to the Alternate Management Network is via a cable connected to a workstation. The Alternate Management Network is accessible only via the dedicated LAN 3 port.

For more information see:

- "*Configuring Direct Connections to RealPresence Collaboration Server (RMX)"* on page **G-1**
- "*Connecting to the Alternate Management Network"* on page **G-6**.

Connection to the *Alternate Management Network* bypasses LAN and Firewall security. Strict control of access to *LAN 3* port is recommended.

Ultra Secure Mode

ULTRA_SECURE_MODE System Flag

The *Ultra Secure Mode* is enabled or disabled depending on the value of the **ULTRA_SECURE_MODE** *System Flag*.

> **WARNING:** Once **Ultra Secure Mode** is enabled it can only be undone by performing a **Restore to Factory Defaults**. Also, to implement a Maximum Security environment, other Polycom products on the network must be similarly configured.
> For more information see "*Restoring Defaults*" on page **J-1**.

In the *Ultra Secure Mode* (**ULTRA_SECURE_MODE =YES**) the enhanced security features of the version are rigorously enforced. The **ULTRA_SECURE_MODE** *System Flag* affects the ranges and defaults of the *System Flags* that control:

- Network Security
- User Management
- Strong Passwords
- Login and Session Management
- Cyclic File Systems alarms

For more information see:

- "*User and Connection Management in Ultra Secure Mode*" on page **15-8**.
- "*Flags Specific to Maximum Security Environments - Ultra Secure Mode*" on page **22-48**.

> When the ULTRA_SECURE_MODE flag is set to YES, Version 7.8 does not include support for:
>
> - Connection to Alternate Management Network via LAN3 port
> - SUPPORT user
> - Auditor user
> - Chairperson user
> - Connections to External Databases
> - IP Sec security protocols
> - ISDN Cascade
> - Serial connection
> - Modem connection
> - MPM cards
> - PCM
> - SIP
> - SIP security (Digest)
> - SIP TLS
> - SNMP
> - SSH server.
> - USB key configuration
> - Web link (Hyperlink in Participant Properties dialog box)
> - QoS with IPv6
> - Recording link
> - PCO (MS-Outlook)

Securing an External Database

TLS 1.0 is used when securing communications between the MCU and an external database. The certificate is installed on the database server and the MCU is the client. When the certificate is installed on the database server, all client requests and responses are transferred via secure port 443.

It is important to verify that the external database application is operating in secure mode before enabling secure external database communications on the MCU. The MCU checks the validity of external database’s certificate before communicating. If there is a certificate error an *Active Alarm* is raised with *Error in external database certificate* in the description field.

To enable secure MCU Communications with an External Database:

4 Set the MCU to communicate with the database server via port 443 by setting the value of the *System Flag* `EXTERNAL_DB_PORT` in *system.cfg* to 443.

For more information see "*Modifying System Flags"* on page **22-1**.

(PKI) Public Key Infrastructure

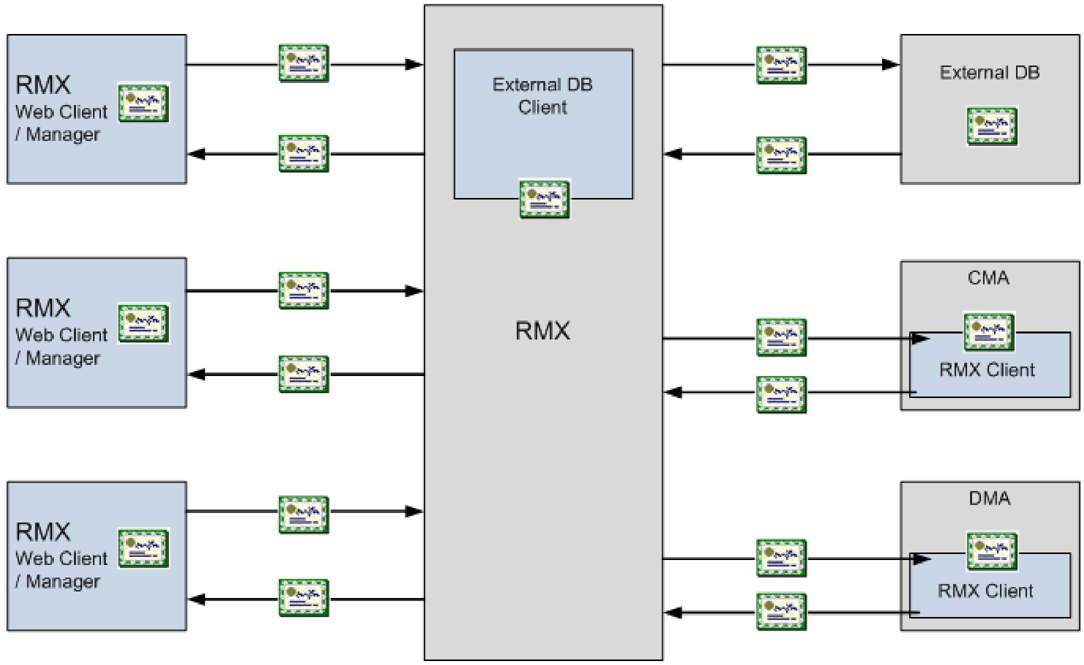
PKI (*Public Key Infrastructure*) is a set of tools and policies deployed to enhance the security of data communications between networking entities.

Unique Certificates for all Networked Entities

The implementation of *PKI* on the MCU has been enhanced to ensure that all networked entities are checked for the presence of unique certificates by implementing the following rules and procedures during the *TLS* negotiation:

- The MCU identifies itself with the same certificate when operating as a server and as a client.
- The MCU’s management applications: *RealPresence Collaboration Server Web Client* and *RMX Manager*, identify themselves with certificates.
- While establishing the required TLS connection, there is an exchange of certificates between all entities.
- Entities such as *CMA* and *DMA* that function as both client and server within the *Management Network* identify themselves with the same certificate for both their client and server functions.

The following diagram illustrates the certificate exchange during the *TLS* connection procedure.



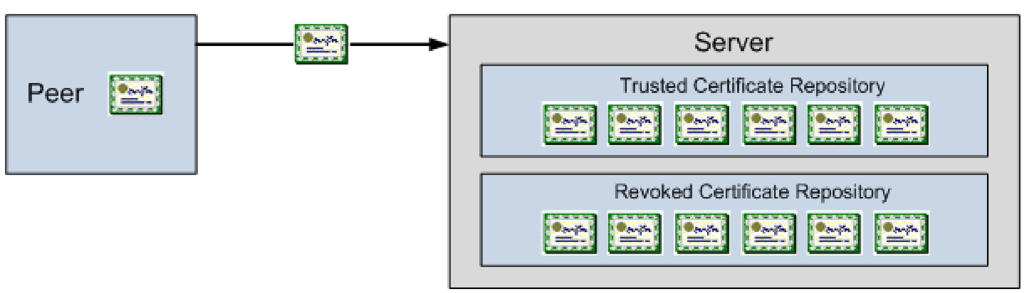
Offline Certificate Validation

Offline Certificate Validation has been enhanced to include the following rules and procedures:

Peer Certificates

The diagram below illustrates the peer certificate validation procedure.

- The credentials of each certificate received from a networked peer are verified against a repository of trusted certificates. (Each networked entity contains a repository of trusted certificates.)
- The digital signature of the certificate's issuing authority is checked along with the certificate's validity (expiration date).



Self Validation of Certificates

- The *DNS* name field in the entity's certificate is checked for a match with the entity's *DNS* name.

- The date of the *MCU's* certificate is checked for validity during power-up and when connecting to management applications (*RealPresence Collaboration Server Web Client* and *RMX Manager*).

Certificate Revocation List

- Each certificate received from a networked peer is verified against a repository of revoked certificates. (Each networked entity contains a repository of revoked certificates.
- Revocation certificates are checked against a list of trusted issuers.
- The digital signature of the issuing authority of the revocation certificate is verified.

Installing and Using Certificates on the MCU

The following certificate file formats are supported:

- *PEM*
- *DER*
- *PKCS#7/P7B*
- *PKCS#12PFX*

Default Management Network

The procedure necessary to purchase and install certificates for the *Default Management Network* of the MCU is unchanged and is described in "*Secure Communication Mode"* on page **F-1**.

Peer Certificate Validation

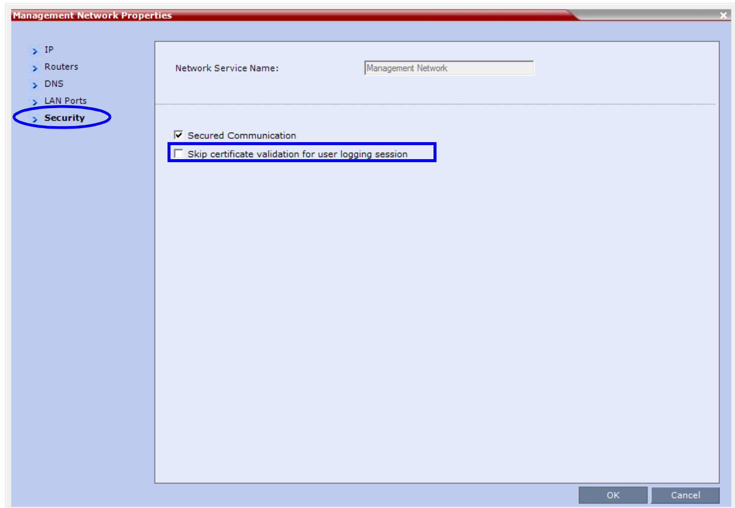
The *Skip certificate validation for user logging session* check box must be cleared when enabling *Secured Mode*. If it is not cleared an *Active Alarm* is created and a message is displayed stating that *Secured Communications Mode* must be enabled.

To enable Request Peer Certificate:

1. In the *RMX Management* pane, click the **IP Network Services** entry.
2. In the *IP Network Services* list pane, double-click the **Management Network** entry.
3. Click the **Security** tab**.**

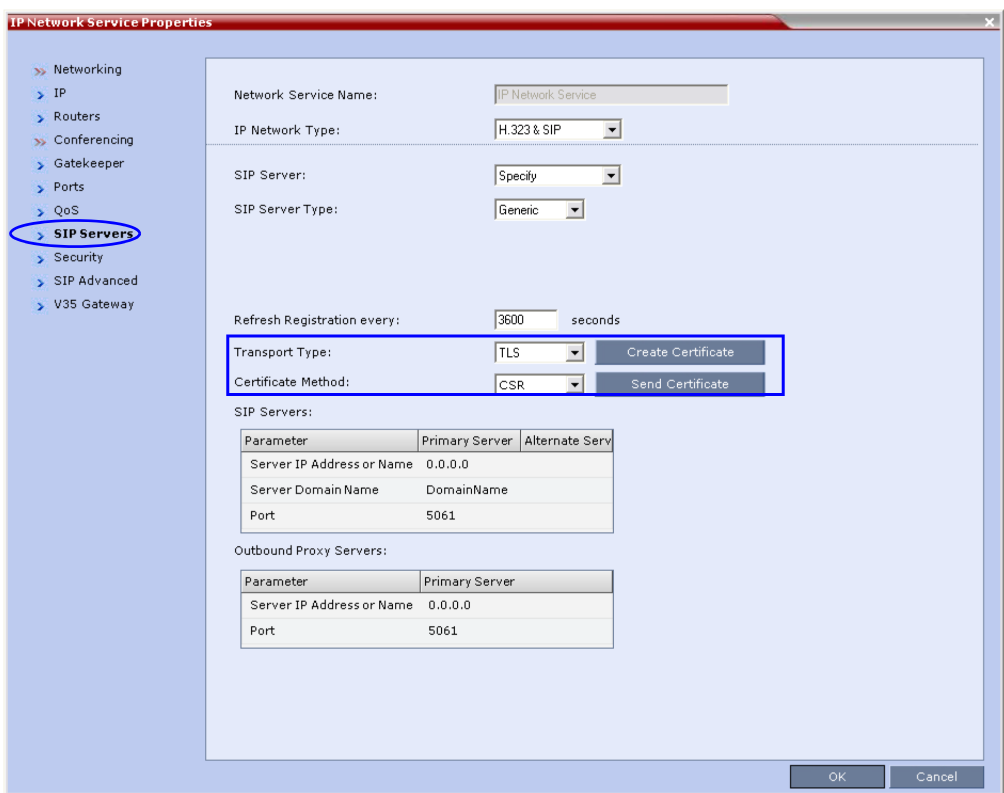
4 Clear the *Skip certificate validation for user logging session* check box.

5 Click the **OK** button.



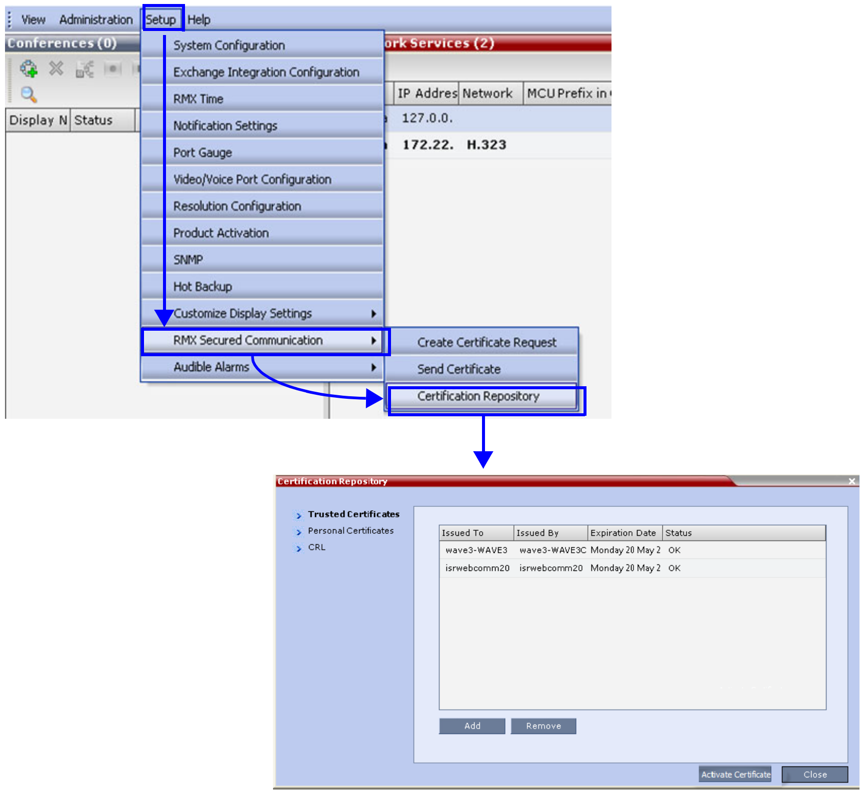
Default IP Network Service

The steps needed to add a certificate to the *Default IP Network Service* are described in the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide,"Modifying the Default IP Network Service"* on page **16-11**.



Managing Certificates in the Certification Repository

A *Certification Repository* dialog box has been added to enable the administrator to add remove and monitor certificates on the MCU. It is accessed via the *RealPresence Collaboration Server Web Client / RMX Manager, Setup* menu.



For information about purchasing certificates see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide*, "*Purchasing a Certificate"* on page **F-2**.

The *Certification Repository* dialog box contains tabs that display the following lists:

- *Trusted Certificates*
- *Personal Certificates (Management and Signaling Certificates)*
- *CRL (Certificate Revocation List)*

Double-clicking on a certificate in any if the displayed lists, displays the certificate's properties:

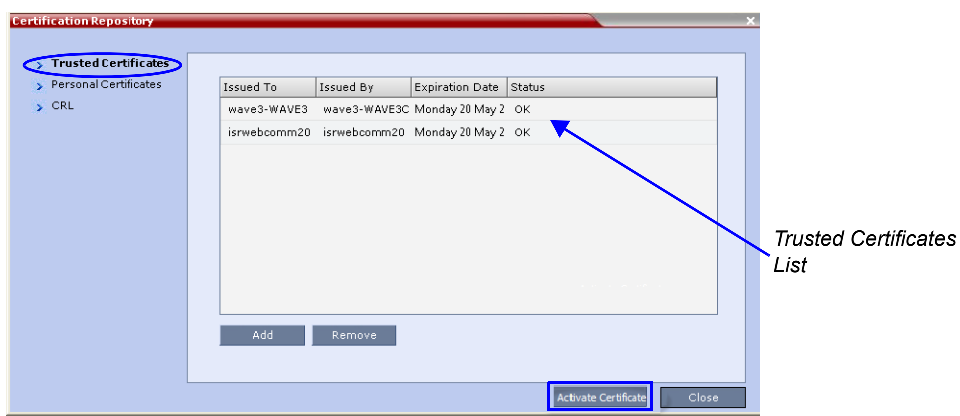
Adding Trusted Certificates and CRLs to the Certification Repository

Trusted Certificates and *CRL*s added to the *Certification Repository* are not automatically activated. They remain in the *Trusted Certificates* and *CRL Lists* until the **Activate Certificate** button is clicked, at which time all *Trusted Certificates* and *CRLs* in the list are activated simultaneously.

Trusted Certificates

By clicking the column headers the *Trusted Certificates* can be sorted by:

- *Issued To*
- *Issued By*
- *Expiration Date*
- *Status*



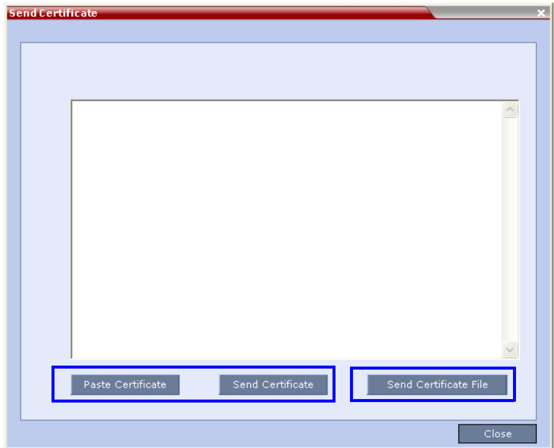
Adding Trusted Certificates

To add a certificate to the repository:

Repeat steps 1 - 4 for each certificate that is to be added to the *Certification Repository*.

1 In the *Trusted Certificates* tab click the **Add** button.

The *Send Certificate* dialog box is displayed.



2 Send the certificate to the MCU.

Two options are available for sending the certificate to the MCU:

— **Paste Certificate and Send Certificate**
Use this option if the certificate has been received from the *Certification Authority* in text format.

— **Send Certificate File**
Use this option if the certificate has been received from the Certification Authority in file format.

Option. Paste Certificate and Send Certificate

After you have received the certificate from the *Certificate Authority:*

a **Copy** (**Ctrl + C**) the certificate information from the *Certificate Authority's* e-mail to the clipboard.

b Click **Paste Certificate** to paste the clipboard content into the *Send Certificate* dialog box.

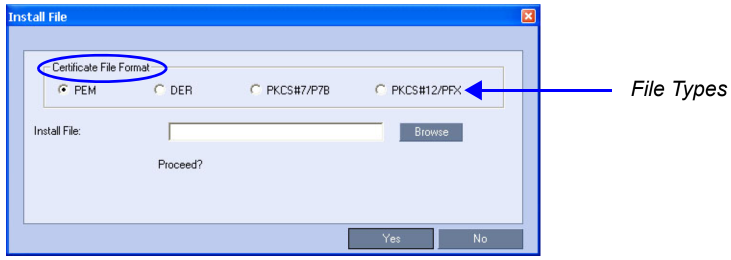
c Click the **Send Certificate** button to send the certificate to the MCU.

Option. Send Certificate File

After you have received the certificate file from the *Certificate Authority:*

a Click **Send Certificate File**.

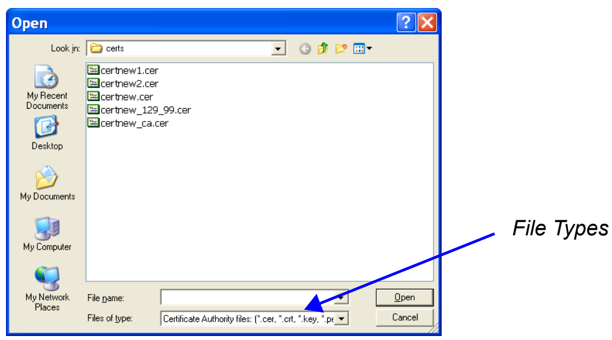
The *Install File* dialog box is displayed.



b Select the *Certificate File Format*: *PEM, DER, PKCS#7/P7B* or *PKCS#12PFX*.

c Enter the certificate file name in the *Install File* field or click the **Browse** button.

The *Open* file dialog box is displayed. The files are filtered according to the file type selected in **Step b**.



d Enter the certificate file name in the *File name* field or click to select the certificate file entry in the list.

e Click the **Open** button.

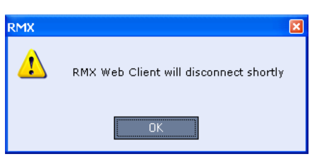
f In the *Install File* dialog box, click the **Yes** button to proceed.

The certificate is added to the *Trusted Certificate List* in the *Certification Repository*.

3 If there are additional *Trusted Certificates* to be added to the *Certification Repository*, repeat steps 1 - 2, otherwise click the **Update Repository** button to complete *Trusted Certificate / CRL* installation.

Before clicking the **Activate Certificate** button ensure that all *CRL*s have also been added to the *Certification Repository*.

When the **Activate Certificate** button is clicked, all added *Trusted Certificates* and *CRL*s are installed and the MCU displays an *RealPresence Collaboration Server (RMX) Web Client/RMX Manager* disconnection confirmation dialog box.



4 Click **OK**.

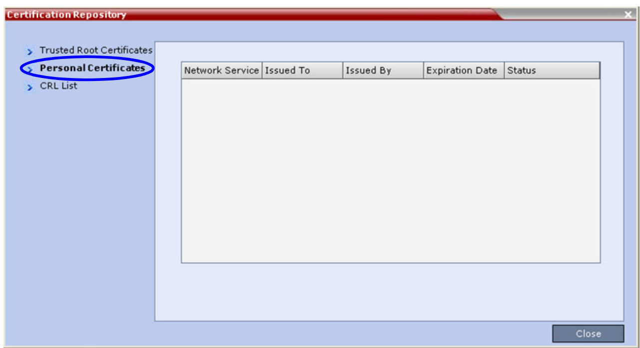
5 Login to the MCU to proceed with further management tasks.

Personal Certificates (Management and Signaling Certificates)

Default Management and *Default IP Network Service* certificates can be viewed in the *Personal Certificates* tab.

They are listed alongside the service to which they are attached. By clicking the column headers the *Trusted Certificates* can be sorted by:

- *Network Service*
- *Issued To*
- *Issued By*
- *Expiration Date*
- *Status*

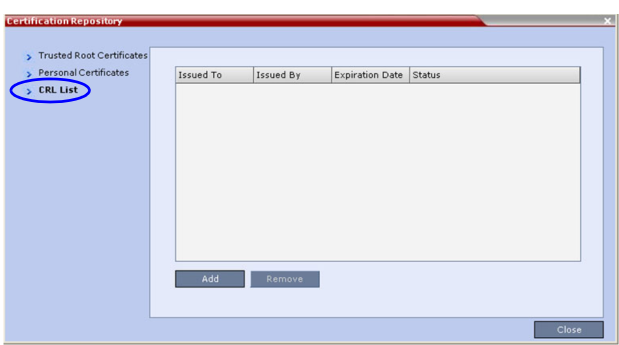


CRL (Certificate Revocation List)

A *CRL* contains a summary of the installed *Certificate Revocation Lists*.

By clicking the column headers the *Certificate Revocation List* can be sorted by:

- *Issued To*
- *Issued By*
- *Expiration Date*
- *Status*



If the *CRL List* is not valid for any reason an *Active Alarm* is created and a message is displayed. The *RealPresence Collaboration Server Web Client/RMX Manager* connection to the MCU is not disabled.

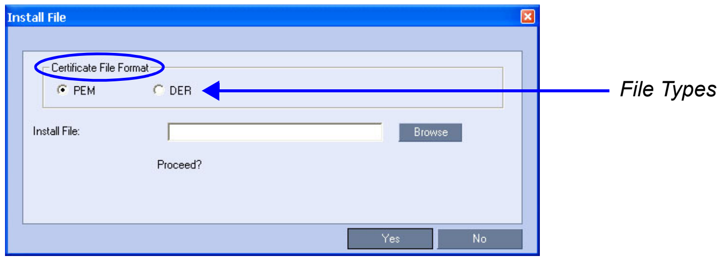
Adding a CRL

To add a CRL to the repository:

Repeat steps 1 - 7 for each *CRL* that is to be added to the *Certification Repository*.

1 In the *CRL List* tab, click the **Add** button.

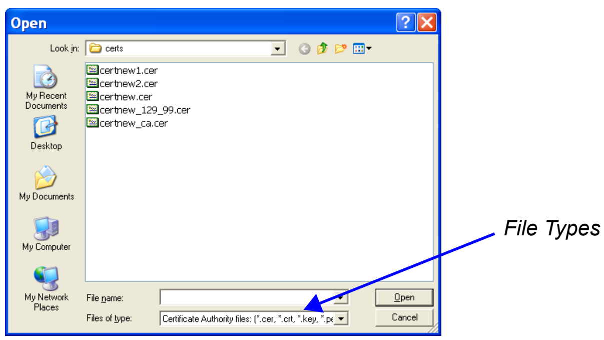
2 The *Install File* dialog box is displayed.



3 Select the *Certificate File Format*: *PEM* or *DER*.

4 Enter the certificate file name in the *Install File* field or click the **Browse** button.

5 The *Open* file dialog box is displayed. The files are filtered according to the file type selected in **Step b**.



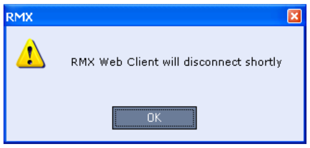
6 Enter the *Certificate* file name in the *File name* field or click to select the certificate file entry in the list.

7 Click the **Open** button.

The certificate is added to the *CRL List* in the *Certification Repository*.

8 If there are additional *CRLs* to be added to the *Certification Repository*, repeat steps 1 - 7, otherwise click the **Activate Certificate** button to complete *CRL / Trusted Certificate* installation.
Before clicking the **Activate Certificate** button ensure that all *Trusted Certificates* have also been added to the *Certification Repository*.

When the **Activate Certificate** button is clicked, all added *Trusted Certificates* and *CRL*s are installed and the MCU displays an *RealPresence Collaboration Server Web Client/RMX Manager* disconnection confirmation dialog box.



9 Click the **OK** button.

10 Login to the MCU to proceed with further management tasks

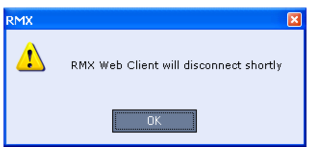
Removing a CRL

To remove a CRL:

1 In the certificate list, select the *CRL List* to be removed.

2 Click the **Remove** button.

The certificate is removed and the MCU displays an *RealPresence Collaboration Server Web Client/Manager* disconnection confirmation dialog box.



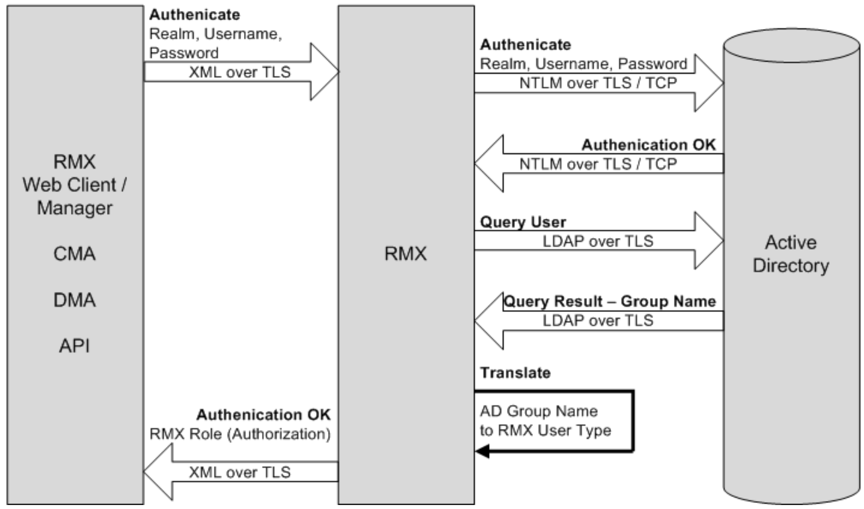
3 Click the **OK** button.

Login to the MCU to proceed with further management tasks.

MS Active Directory Integration

It is possible to configure direct interaction between the MCU and *Microsoft Active Directory* for *Authentication* and *Authorization* of *Management Network* users.

The following diagram shows a typical user authentication sequence between a *User*, MCU and *Active Directory*.



Directory and Database Options

Ultra Secure Mode

Internal MCU database and Active Directory

Authentication is first attempted using the internal MCU database. If it is not successful authentication is attempted using the *Active Directory*.

Standard Security Mode

Internal MCU database + External Database

First authentication is via the internal MCU database. If it is not successful, authentication is via the *External Database*.

Internal MCU database + External Database + Active Directory

- **Management Logins**

  First authentication is via the internal MCU database. If it is not successful, authentication is via the *Active Directory*.

- **Conference Queries** (*Chairperson Password, Numerical ID* etc.)

  First authentication is via the internal MCU database. If it is not successful, authentication is via the *External Database*.

Guidelines

- The MCU maintains a local record of:
  - *Audit Events* – users that generate these events are marked as being either internal or external.
  - Successful user logins
  - Failed user login attempts
- User passwords and user lockout policy for external users are managed via *Active Directory's* integration with the user's host machine.
- Enabling or disabling *Active Directory* integration does not require a reset.

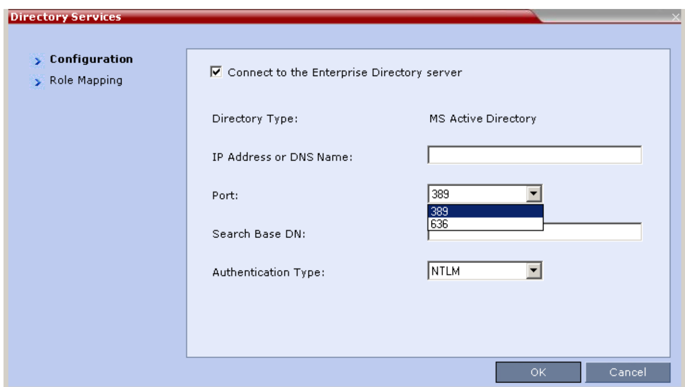
- In *Standard Security Mode* multiple accounts of all user types are supported. In *Ultra Secure Mode*, enabling *Active Directory* integration is only permitted if the MCU only has one local *Administrator User*.
- Multiple *Machine Accounts* with various roles are supported.
- *Microsoft Active Directory* is the only directory service supported.
- *Active Directory* integration is configured as part of the *Management Network*.
- Both *IPv4* and *IPv6* addressing are supported.
- In *Standard Security Mode,* the *Active Directory* can be queried using *NTLM* with or without *TLS* encryption. In *Ultra Secure Mode, TLS* encryption is required.
- Server and client certificate validation requests use *LDAP* with or without *TLS* encryption.

> When using *LDAP* over *TLS*, in addition to using port **389** with *STARTTLS*, the administrator has the option of using port **636**.

Enabling Active Directory Integration

To configure Directory Services:

1. On the *RMX Menu*, click **Setup > Directory Services**.
   The *Directory Services - Configuration* dialog box is displayed.



2. Modify the following fields.

Table F-4 Directory Services - Configuration

Field	Description
Connect to the Enterprise Directory Server	Select this check box to enable or disable the *Active Directory* feature.
IP Address or DNS Name	Enter the IP address or DNS name of the Enterprise Directory Server (Active Directory).
Port	Select the *Port* according to the *Authentication Protocol* to be used: • **389** - *NTLM* over *TCP* • **636** - *NTLM* over *TLS*

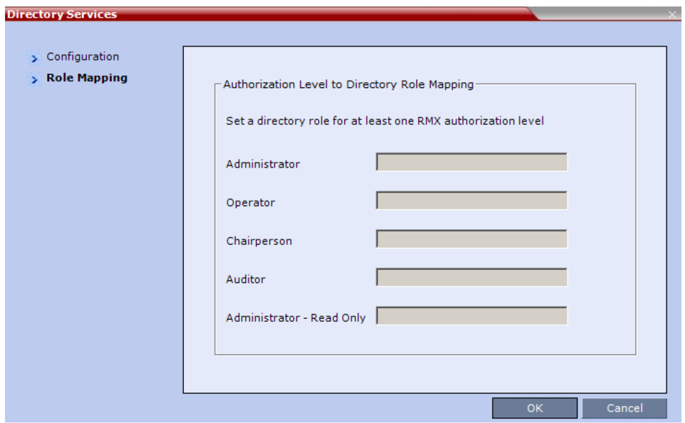
***Table F-4** Directory Services - Configuration (Continued)*

Field	Description

Search Base DN	Enter the starting point when searching for *User* and *Group* information in the *Active Directory*.
	For example if the *Domain Name* is:
	`mainoffice.bigcorp.com.uk`
	The entry in this field should be:
	`CN=Users,DC=mainoffice,DC=bigcorp,DC=come,DC=uk`

Authentication Type	Only NTLM can be used.

3 Click the **Role Mapping** tab.
The *Directory Services - Role Mapping* dialog box is displayed.



Each of the MCU user types: *Administrator*, Administrator Read-Only, *Auditor*, *Operator* and *Chairperson* can be mapped to only one *Active Directory Group* or *Role* according to the customer's specific implementation.

— In *Ultra Secure Mode* there are only two user types: *Operator* and *Administrator*.

— An MCU user that belongs to multiple *Active Directory Groups* is assigned to the *Group* with the least privileges.

4 Map the *MCU User Types,* to their *Active Directory* roles by modifying the following fields.

***Table F-5** Directory Services - Role Mapping*

Field	Description
Administrator	At least one of these *User Types* must be mapped to an *Active Directory Role*.
Administrator Read-Only	
Operator	
Chairperson	
Auditor	

5 Click **OK**.

Restoring the RealPresence® Collaboration Server (RMX®) 1500/2000/4000 Using the USB Port

When the RMX is in *Ultra Secure Mode*, the *Restoring the RealPresence® Collaboration Server Using the USB Port* procedure can be used to set the RMX back to its factory default settings, if for any combination of factors the system becomes unstable or unmanageable.

For more information see "*Ultra Secure Mode"* on page **F-7**.

For a full description of this procedure see the *Polycom® RealPresence® Collaboration Server (RMX®) 1500/2000/4000 Deployment Guide for Maximum Security Environments*, "*Restoring the RealPresence® Collaboration Server (RMX®) 1500/2000/4000 Using the USB Port"* on page **4-1**.

Appendix G

Configuring Direct Connections to RealPresence Collaboration Server (RMX)

Direct connection to the RealPresence Collaboration Server (RMX) is necessary if you want to:

- Modify the MCU's *Factory Default Management Network* settings without using the USB key.
- Connect to the MCU's *Alternate Management Network* for support purposes.
- Connect to the MCU via a modem.

> Direct connections to the MCU are not supported when the MCU is in *Ultra Secure Mode*.
> For more information see "*Ultra Secure Mode*" on page **F-7**.

Management Network (Primary)

If you do not want to use the USB key method of modifying the MCU's *Management Network* parameters, it is necessary to establish a direct connection between a workstation and the MCU.

Alternate Management Network

The *Alternate Management Network* enables direct access to the MCU for support purposes.

While being separate from all other networks, it has identical functionality to the *Management Network*.

Support personnel can log in and use it to manage the MCU if a connection to the *Management Network* cannot be made or if internet access to the host network is blocked by LAN security or a firewall.

The *Alternate Management Network* cannot be configured and operates according to factory defaults.

The administrator's **Login** name, **Password**, viewing and system permissions on the *Alternate Management Network* are the same as those on the *Management Network.*

Once logged in, the *RealPresence Collaboration Server Web Client* behaves as if the administrator had logged in on the *Management Network*.

> Connection to the *Alternate Management Network* bypasses LAN and Firewall security. Strict control of access to *LAN 3* port is recommended.

> The *Alternate Management Network* is only available if *Network Separation* has not been performed. For more information, see "*Multiple Network Services"* on page **16-49**.

Configuring the Workstation

The following procedures show how to modify the workstation's networking parameters using the *Windows New Connection Wizard*.

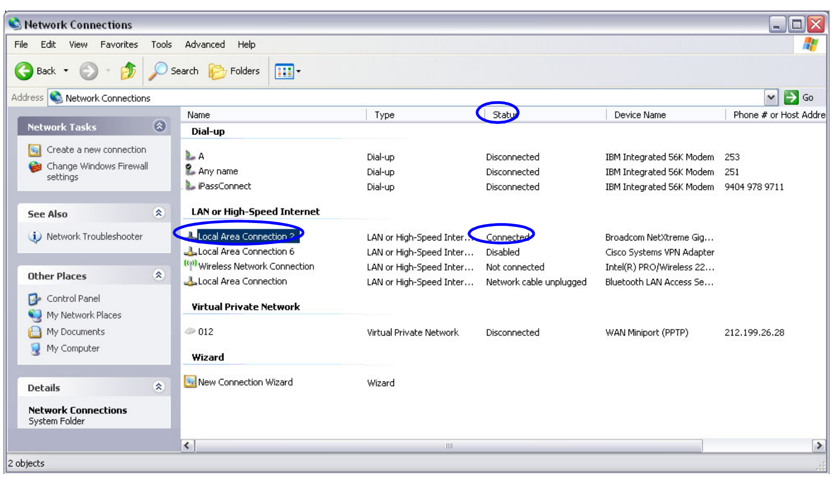
For non-Windows operating systems an equivalent procedure must be performed by the system administrator.

Before connecting directly, you must modify the *IP Address*, *Subnet Mask* and *Default Gateway* settings of the workstation to be compatible with either the MCU's *Default Management Network* or *Alternate Management Network*.

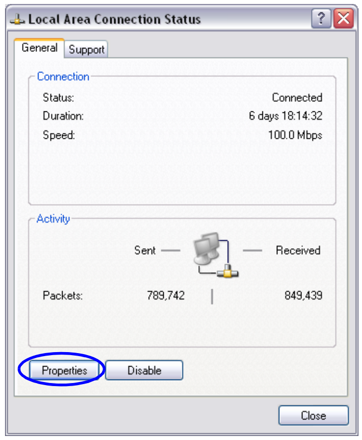
To modify the workstation's IP addresses:

1 On the Windows *Start* menu, select **Settings** > **Network Connections.**

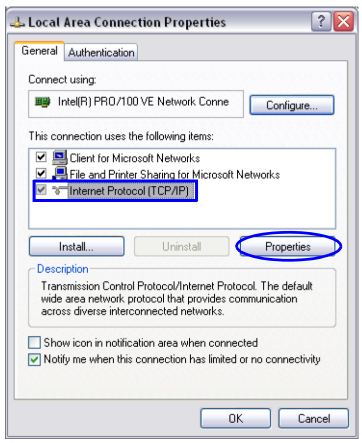
2 In the *Network Connections* window, double-click the **Local Area Connection** that has *Connected* status.



3 In the *Local Area Connection Status* dialog box, click the **Properties** button.

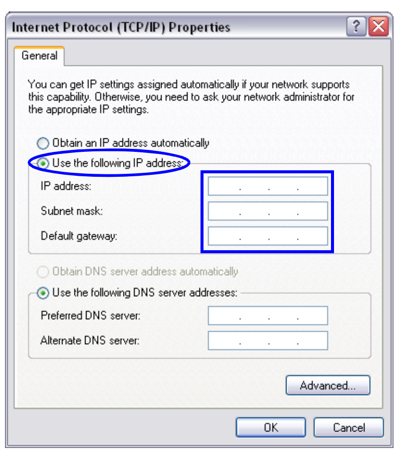


4 In the *Local Area Connection Properties* dialog box, select **Internet Protocol [TCP/IP]** > **Properties**.



5 In the *Internet Protocol (TCP/IP) Properties* dialog box, select **Use the following IP address**.

6 Enter the *IP address, Subnet mask* and *Default gateway* for the workstation.



The workstation's IP address should be in the same network neighborhood as the MCU's *Control Unit* IP address.

Example: *IP address* – near **`192.168.1.nn`**

None of the reserved IP addresses listed in *Table G-1* should be used for the IP Address.

The *Subnet mask* and *Default gateway* addresses should be the same as those for the MCU's *Management Network*.

The addresses needed for connection to either the MCU's *Default Management Network* or *Alternate Management Network* are listed in Table G-1.

For more information about connecting to the *Alternate Management Network*, see "*Connecting to the Alternate Management Network"* on page **G-6**.

Table G-1 *Reserved IP Addresses*

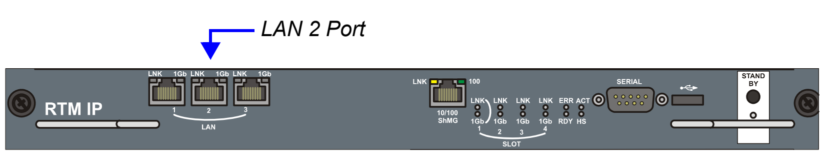
Network Entity	IP Address	
	Management Network (Factory Default)	Alternate Network
Control Unit IP Address	192.168.1.254	169.254.192.10
Control Unit Subnet Mask	255.255.255.0	255.255.240.0
Default Router IP Address	192.168.1.1	169.254.192.1
Shelf Management IP Address	192.168.1.252	169.254.192.16
Shelf Management Subnet Mask	255.255.255.0	255.255.240.0
Shelf Management Default Gateway	192.168.1.1	169.254.192.1

7 Click the **OK** button.

Connecting to the Management Network

To connect directly to the MCU:

1 Using a LAN cable, connect the workstation to the LAN 2 Port on the MCU's back panel.

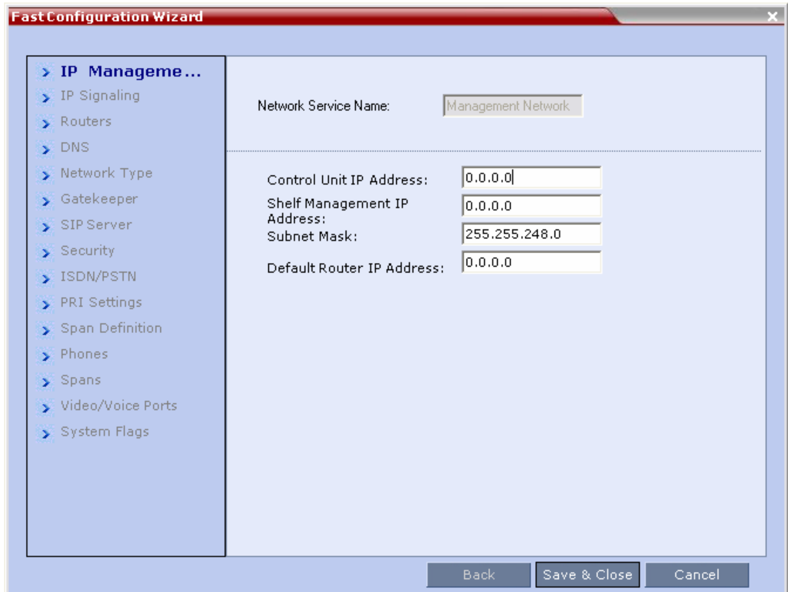


2 Connect the power cable and power the MCU **On**.

3 Start the *RealPresence Collaboration Server Web Client* application on the workstation, by entering the factory setting *Management IP* address in the browser's address line and pressing **Enter**.

4 In the *RealPresence Collaboration Server Web Client* Login screen, enter the default *Username* (**`POLYCOM`**) and *Password* (**`POLYCOM`**) and click the **Login** button.

The *Fast Configuration Wizard* starts.



If no *USB key* is detected and **either**: this is the *First Time Power-up* **or** the *Default IP Service* has been deleted and the MCU has been reset, the following dialog box is displayed:

For more information about First-time Power-up and the *Fast Configuration Wizard* see the *RealPresence Collaboration Server 1500/2000/4000 Getting Started Guide*, "*Procedure 1: First-time Power-up"* on page 2-25.

5 Enter the following parameters using the information supplied by your network administrator:

— *Control Unit IP Address*

— *Shelf Management IP Address*

— *Control Unit Subnet Mask*

— *Default Router IP Address*

6 Click the **Save & Close** button.

The system prompts you to sign in with the new *Control Unit IP Address.*

7 Disconnect the LAN cable between the workstation and the LAN 2 Port on the MCU's back panel.

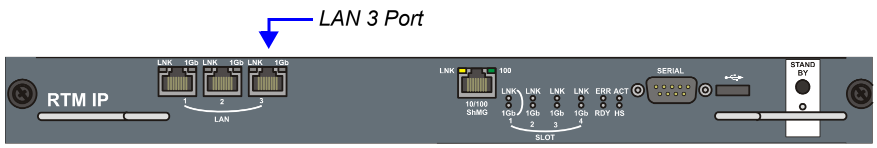
8 Connect LAN 2 Port on the MCU's back panel to the local network using a LAN cable.

9 Enter the new *Control Unit IP Address* in the browser's address line, using a workstation on the local network, and press **Enter** to start the *RealPresence Collaboration Server Web Client* application.

10 In the *RealPresence Collaboration Server Web Client* Login screen, enter the default *Username* (**POLYCOM**) and *Password* (**POLYCOM**) and click the **Login** button.

Connecting to the Alternate Management Network

Access to the *Alternate Management Network* is via a cable connected to a workstation. The *Alternate Management Network* is accessible only via the dedicated *LAN 3* port.



To connect to the Alternate Management Network:

1 Connect the cable between the MCU's LAN 3 port and the LAN port configured on the workstation.

2 Start the *RealPresence Collaboration Server Web Client* application on the workstation, by entering `http://169.254.192.10` (the *Control Unit IP Address*) in the browser's address line and pressing **Enter**.

   The *Login* dialog box is displayed.

3 In the *RealPresence Collaboration Server Welcome Screen*, enter the administrator's *Username* and *Password* and click the **Login** button.

   The *RealPresence Collaboration Server Web Client* starts and the MCU can be managed in the same manner as if you had logged on the *Management Network*.

Connecting to the MCU via Modem

Remote access to the MCU's *Alternate Management Network* is supported via an external PSTN <=> IP modem.

To connect via modem to the *Alternate Management Network* the following procedures must be performed:

1. **Procedure 1: Install the RMX Manager –** the web client enables direct access to the MCU for support purposes.
2. **Procedure 2: Configure the modem** – by assigning it an IP address on a specific subnet in the *Alternate Management Network*.
3. **Procedure 3: Create a dial-up connection –** using the *Windows New Connection Wizard.*
4. **Procedure 4: Connect to the MCU –** via the *RMX Manager*.

Procedure 1: Install the RMX Manager

Before installing the *RMX Manager*, verify that you have at least 150Mb of free space on your workstation.

For more information see "*Installing the RMX Manager"* on page 20-2.

Procedure 2: Configure the Modem

Configure the modem as follows:

- **IP address** – near `169.254.192.nn`
- **Subnet Mask** – `255.255.240.0`

> None of the reserved IP addresses listed in Table G-1 on page G-4 should be used for the IP Address.

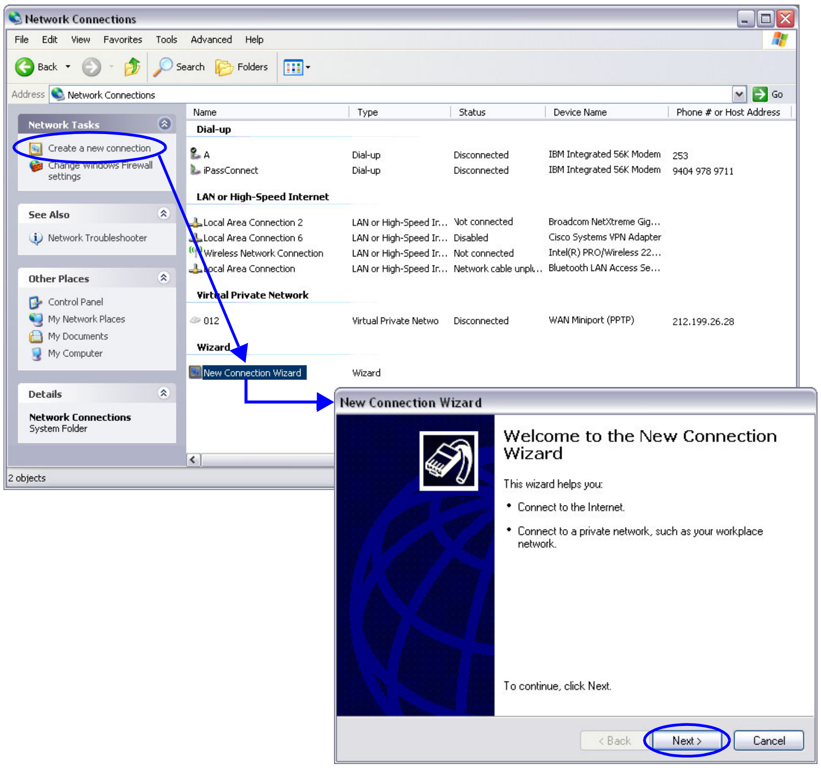
Procedure 3: Create a Dial-up Connection

To create a dial-up connection:

This procedure is performed once. Only the *Dial* field in the *Connect* applet (see step 10 on page **G-11**) is modified for connection to different modems.

1 In *Windows*, navigate via the *Control Panel* to the *Network Connections* applet and select **Create a new connection.**

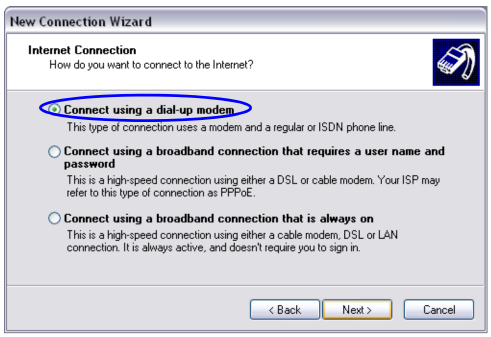
2 When the *New Connection Wizard* is displayed, click the **Next** button.



3 In the *Network Connection Type* box, select **Connect to the Internet** and click the **Next** button.

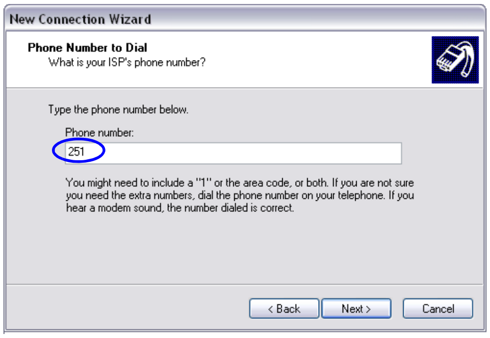
4 In the *Getting Ready* box, select **Set up my connection manually** and click the **Next** button.

5 In the *Internet Connection* box, select **Connect using dial-up modem** and click the **Next** button.



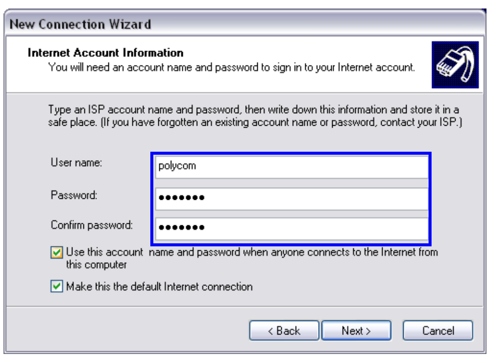
6 In the *Connection Name* box, enter a **Name** for the modem connection (e.g. *Modem Connection*) and click the **Next** button.

7 In the *Phone Number to Dial* box, enter the **Phone Number** for the modem and click the **Next** button.

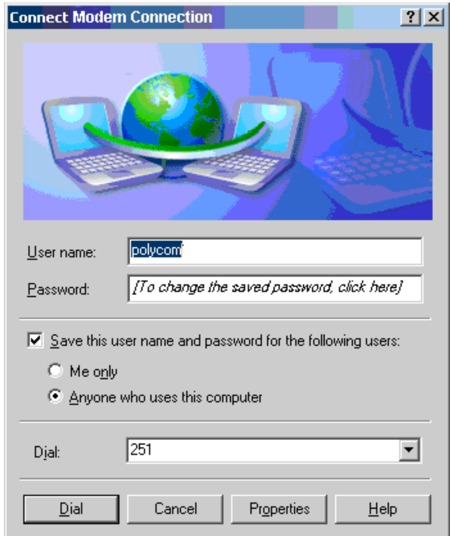


8 In the *Connection Availability* box, select **Anyone's use** and click the **Next** button.

9 In the *Internet Account Information* box, complete the *Username*, *Password* and *Confirm Password* fields and click the **Next** button.

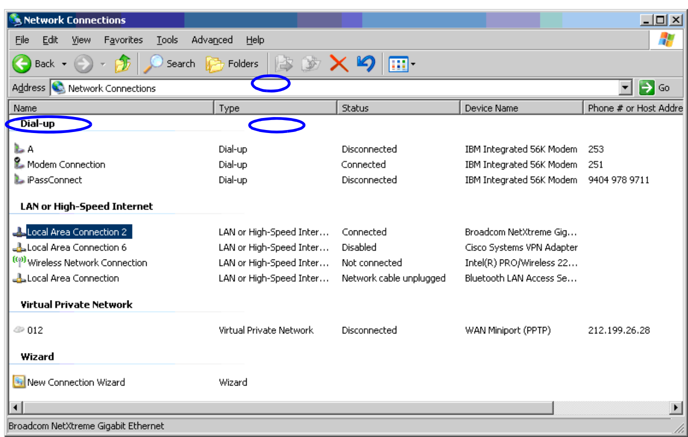


10 The *Connection* applet is displayed with the field values filled in as specified by the *New Connection Wizard*.



11 Click the **Dial** button to establish a connection to *LAN 3 Port* via the modem.

The *Windows – Network Connections* applet displays *Connected* status for the new connection.



Procedure 4: Connect to the MCU

To Connect using the RMX Manager:

To use the browser:

4 In the browser's command line, enter **`http://<MCU Control Unit IP Address>/RmxManager.html`** and press **Enter**.

To use the Windows Start menu:

1 Click **Start.**

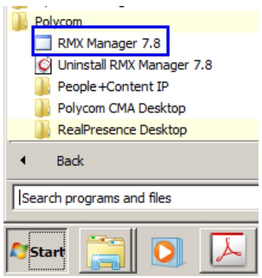
a If the *MCU Manager* is displayed in the recently used programs list, click RMX **Manager** in the list to start the application.

or

b Click **All Programs.**

The *All Programs* list is displayed.

a Select **Polycom** and then select **RMX Manager**.



The *RMX Manager – Welcome* screen is displayed.

Appendix H

Setting the MCU for Integration Into Microsoft Environment

Integration into Microsoft environment (using Lync endpoints) is supported in AVC Conferencing Mode only.

Overview

The Polycom® Visual Communications offers high quality video and audio multipoint conferencing by integrating the Polycom network devices and endpoints into Microsoft® platforms. The Polycom® RealPresence® Collaboration Server (MCU) system can be integrated into the following Microsoft environments:

- Office Communications Server 2007 environment (Microsoft R2, Wave 13)
- Lync Server 2010 environment (Microsoft Wave 14)

From Version 7.0.x, Microsoft R1 is not supported with MCU systems.

Point-to-point and multipoint audio and video meetings can be initiated from Office Communicator/Lync client, Windows Messenger and Polycom video endpoints (HDX and VSX) when the environment components are installed and configured.

Multipoint calls are enabled when the MCU is installed in the Microsoft environment and is configured for unified communications. Routing to conferences can be performed by the Office Communications Server/Lync Server either by:

- *Matched URI dialing* - using the SIP URI address (both Office Communications Server and Lync Server)
- *Numerical dialing* - enables a common dialing plan for Meeting Rooms across Office Communications Server and H.323 infrastructures (not available in Lync server environment).

Only TLS connections to the MCU will work, TCP connections will not work.
The RMX does not support working with multiple Edge servers.

TLS certificates can be generated using the following methods: CSR, PFX and PEM; each giving different options for *Encryption Key* length. Table H-1 lists the *SIP TLS Encryption Key* length support for the various system components.

Table H-1 *SIP TLS - Encryption Key Support by System Component*

System Component	Key Generation Method	Key Length (bits)	Key generated by
SIP Signaling	CSR	2048	MCU
	PFX / PEM	1024 or 2048	User
Management	CSR	2048	MCU
LDAP			

Conferencing Entities Presence

Conferencing entities (Meeting Rooms, Entry Queues and SIP Factories) can be registered with the SIP server (Office Communication Server or Lync server) enabling the addition of these conferencing entities to the buddy list while displaying their presence (availability status: Available, Offline, or Busy). Office Communication Server client or Lync Server client users can connect to conferencing entities directly from the buddy list.

The configuration of the environment to enable Presence, is usually done once the basic configuration is completed.

For more details, see "*Adding Presence to Conferencing Entities in the Buddy List"* on page **H-51**.

Multiple Networks

A more complex configuration, in which two Microsoft SIP servers are used (one Lync Server and one Office Communications Server) is also supported using the MCU Multiple Networks configuration.

In this configuration, each Microsoft SIP Server is defined in a Network Service of its own (in this case two IP Network Services are defined). A DNS server can be specified for each IP Network Service and for the RMX Management Network Service.

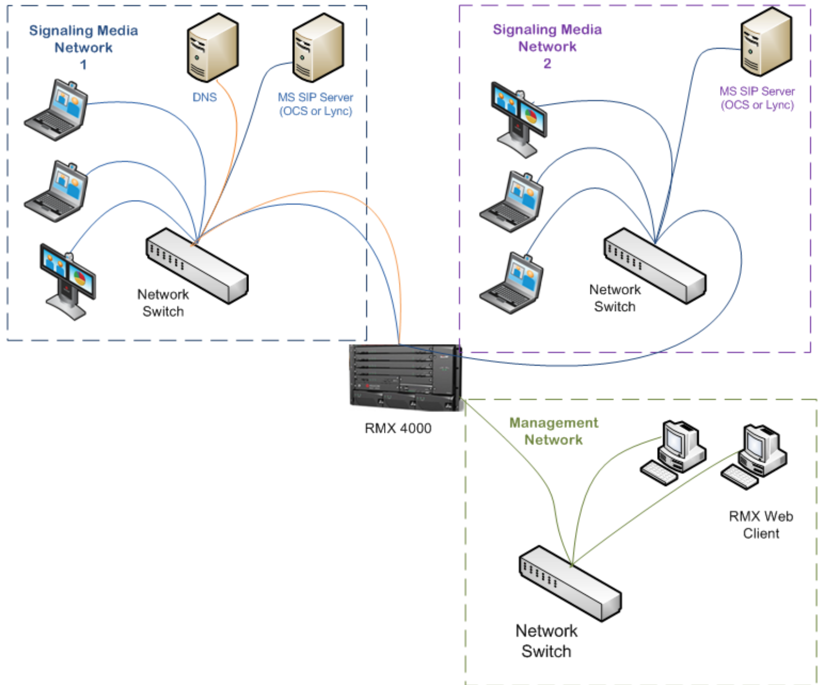


Figure H-1 *MCU Multiple Networks Topology*

ICE is supported with this configuration from *Version 7.8* onward.

One *Network Service* including *ICE* can be configured per media card installed in the MCU as shown in Table H-2.

Table H-2 *RMX - Media Cards vs Network Services including ICE*

RMX	Total Media Cards	Network Services (Up to 2 per Media Card)	Network Services that Include ICE (1 per Media Card)
1500	1	2	1
2000	2	4	2
4000	4	8	4

Guidelines

- If *ICE* initialization fails in a *Network Service*:
  — The *Network Service* remains functional but without *ICE* capability.
  — *ICE* capability on media cards that share the same *Network Service* also remain functional but without *ICE* capability.
  — Other *Network Services* with *ICE* capability on other media cards are unaffected.
- A *DNS* server can be specified for each *IP Network Service* and for the MCU *Management Network Service*.

For more details about Multiple Networks configuration, see "*Multiple Network Services"* on page **16-49**.

Interactive Connectivity Establishment (ICE)

Interactive Connectivity Establishment (ICE) provides a structure/protocol to unify the various NAT Traversal techniques that are used to cross firewalls.

It enables SIP based endpoints to connect while traversing a variety of firewalls that may exist between the calling endpoint (local) and the MCU or called endpoint (remote). It is the only way for remote Microsoft Office Communicator/Lync users to call into the enterprise without a VPN.

ICE Guidelines

- ICE is available in *MPM+ Card Configuration Mode* (Version 7.0 and later) and *MPMx Card Configuration Mode* (Version 7.1 and later).
- RMX ICE implementation complies with Microsoft ICE implementation.
- ICE is available only in IPv4 environment.
- ICE can be implemented in an environment that includes a STUN server and a Relay server (for example, Microsoft AV Edge server).
- The firewall must be UDP enabled.

When ICE over UDP is blocked in the firewall UDP port, the ICE connection through the TCP protocol is automatically used instead of UDP for fallback.

- The MCU must have a unique account in the Active Directory and must be registered with the Office Communications/Lync server.
- From *Version 7.8*, ICE is supported with MCU Multiple Networks.
- Ensure that the MCU system SIP signaling domain has been allowed on the Lync Server edge server to which you are federating (if your deployment does not include a DMA system).
- Content sharing (BFCP protocol) is not supported in ICE environment.

Connecting to the MCU in ICE Environment

The dialing methods that can be used by an endpoint to connect to another endpoint depends on the ICE environment: Local, Remote or Federation.

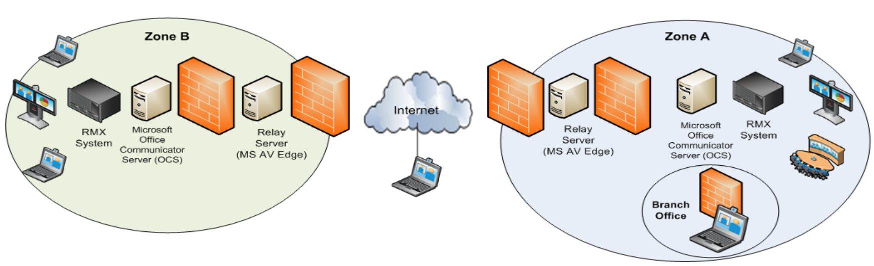


Figure H-2 *ICE Environment*

Local connection - a connection between the MCU and endpoints that reside within the same organization. For example, an endpoint in Zone A calls the MCU in Zone A.

Branch Office - a connection between an endpoint that is behind a firewall and the MCU that reside in the same zone. The user in the Branch Office can also place and receive calls from other enterprises and remote users. For example, Enterprise A also contains a branch office, which in this example is a Polycom HDX user who is behind more than one firewall.

Remote - a connection between MCU that resides within the organization and an endpoint that resides outside of the organization (on a WAN). For example, an endpoint on the internet that calls the MCU in Zone A. In such a case, the call has to traverse at least one firewall.

Federation - a connection between MCU that resides within one organization and an endpoint that resides within another organization. For example, an endpoint in Zone A calls the MCU in Zone B. The call has to traverse two or more firewalls.

Dialing Methods

The ICE protocol enables remote and federation connections using the registered user name for dialing. The endpoint connects to the MCU by entering the MCU registered user name in the following format:

[MCU registered user name]@[OCS/Lync server domain name]

For example: **rmx111@ilsnd.vsg.local**

The call reaches the Transit Entry Queue of the MCU and via IVR is routed to the destination conference.

This method is added to the local connections and *Matched URI* and *Numerical Dialing* methods available in Microsoft Office Communication environment and the *Numerical Dialing* method available in the Lync server environment.

The following table summarizes the dialing methods and its availability in the various configurations.

Table H-3 *Available dialing methods per Connection Type*

	Matched URI Routing	Numerical Dialing	Registered User Name
Local	√	√	√
Branch office	√*	X	√
Remote	√*	X	√
Federation	√*	X	√

* To enable the *Matched URI dialing* in the federated environment to be able to connect to the MCU SIP signaling domain, you must also configure the Office Communications Server/Lync Server.

When federating an Office Communications Server/Lync Edge server with another Office Communications Server/Lync server environment, you need to include the FQDN of the Office Communications Server/Lync Edge server as well as the SIP signaling domain for federated environment. The SIP signaling domain is the FQDN of the Polycom DMA system or a Polycom MCU system (when your deployment does not include a DMA system).

For example, if company B wants to set up federation with company A and receive and send SIP calls that will be handled by the Polycom SIP signaling domain in company A, you need to add the FQDN of the company A Office Communications Server domain as well as the SIP signaling domain of company A to the list of internal SIP Server domains supported by the company B Office Communications Server/Lync Server environment.

For more information, see the Microsoft documentation and the *Polycom® Unified Communications Deployment Guide for Microsoft® Environments*.

Integrating the MCU into the Microsoft Office Communications Server Environment

From Version 7.0.x, Microsoft R1 is not supported with MCU systems.

When the MCU is integrated into the Office Communications Server environment, calls to conferences running on the MCU can be routed using Matched URI dialing and/or Numerical dialing.

Both routing methods (numerical dialing and Matched URI dialing) can be enabled simultaneously in the Office Communications Server and the MCU system or you can enable one of these methods, depending on your environment requirements.

In both methods, the MCU configuration is the same.

Setting the Matched URI Dialing Method

To enable the Matched URI dialing method the following tasks have to be completed:

Office Communications Server side:

1 Set the Static Route & Trusted Host for MCU in the Office Communications Server.

2 **Optional if Load Balancer Server is present.** Set the Static Route & Trusted Host for MCU in the Load Balancer server.

MCU side:

The following tasks are detailed in "*Configuring the RMX 1500/2000/4000 for Microsoft Integration*" on page **H-36**.

3 Modify the Management Network Service to include the DNS server and set the Transport Type to TLS.

4 Create the security certificate (using one of the two available methods)

5 Define a SIP Network Service in the MCU and install the TLS certificate.

6 Modify and add the required system flags in the MCU System Configuration.

7 **Optional.** Defining additional Entry Queues and Meeting Rooms in the MCU environment. For more information see "*Defining a New Entry Queue*" on page **7-3** and "*Creating a New Meeting Room*" on page **6-4**.

For a detailed description of the configuration of the Polycom conferencing components for the integration in Microsoft Office Communications Server 2007 see *Polycom® HDX and MCU™ Systems Integration with Microsoft Office Communications Server 2007 Deployment Guide*.

In ICE environment, to enable the Matched URI dialing in the federated environment to be able to connect to the MCU SIP signaling domain, you must also configure the Office Communications Server. When federating an Office Communications Server edge server with another Office Communications Server environment, you need to include the FQDN of the Office Communications Server edge server as well as the SIP signaling domain for federated environment. The SIP signaling domain is the FQDN of the Polycom DMA system or a Polycom MCU system (when your deployment does not include a DMA system).

Note: The RMX does not support working with multiple edge servers.

For example, if company B wants to set up federation with company A and receive and send SIP calls that will be handled by the Polycom SIP signaling domain in company A, you need to add the FQDN of the company A Office Communications Server domain as well as the SIP signaling domain of company A to the list of Internal SIP Server domains supported by the company B Office Communications Server environment.

For more information, see the Microsoft documentation and the *Visual Communications Deployment Administration Guide*.

Configuring the Office Communications Server for MCU Systems

To be able to work with the Office Communications Server, the MCU unit must be configured as a Trusted Host in the OCS. This is done by defining the IP address of the signaling host of each MCU unit as Trusted Host.

Meeting Rooms are usually not registered to the OCS, and Static Routes are used instead. Setting Static Routes in the OCS enables SIP entities / UAs to connect to conferences without explicit registration of conferences with the OCS.

Routing is performed by the OCS based on the comparison between the received URI and the provisioned static route pattern. If a match is found, the request is forwarded to the next hop according to the defined hop's address.

This is the recommended working method. It alleviates the need to create a user account in the OCS for each Meeting Room and Entry Queue. This also allows users to join ongoing conferences hosted on the MCU without registering all these conferences with OCS.

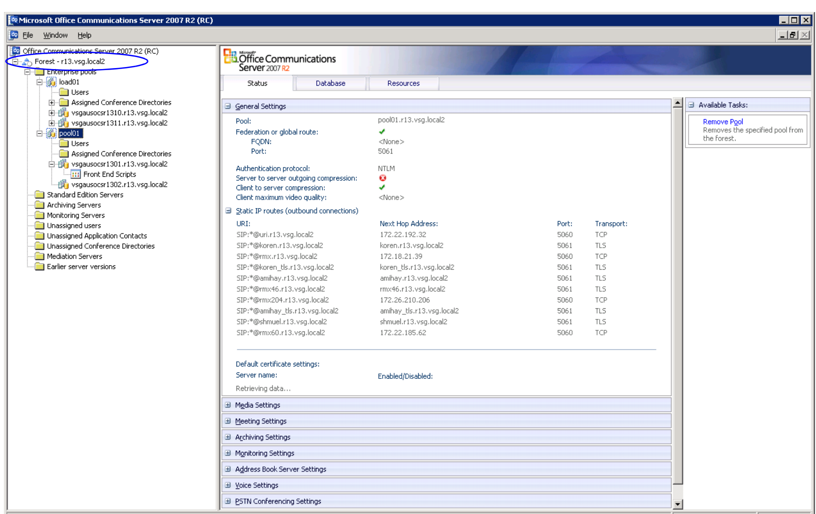
Entry Queues can also be for Ad-hoc conferencing enabling Office Communicator clients to dial to the Entry Queue and create a new ongoing conference using DTMF codes to enter the target conference ID. In such a case, other OC users will have to use that ID to join the newly created conference.

Setting the Trusted Host for MCU in the Office Communications Server

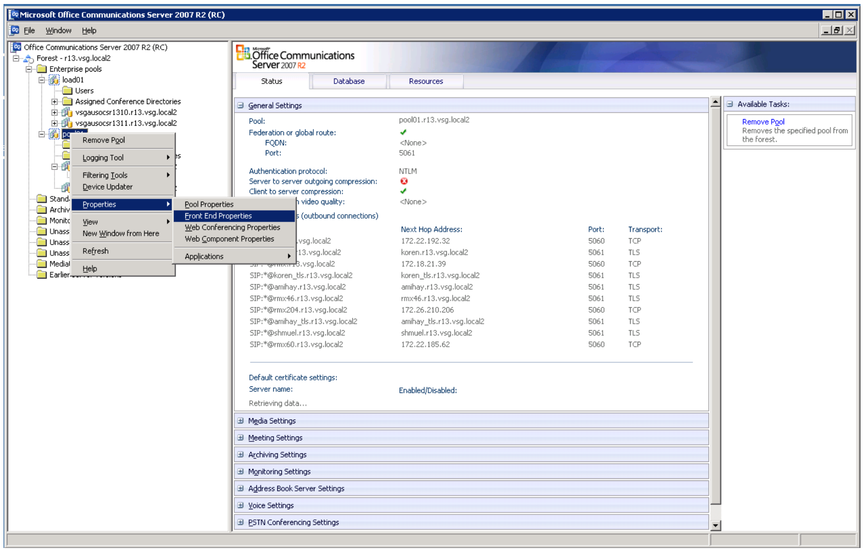
To set the MCU as trusted in OCS:

1 Open the OCS Management application.

2 Expand the *Enterprise Pools* list.

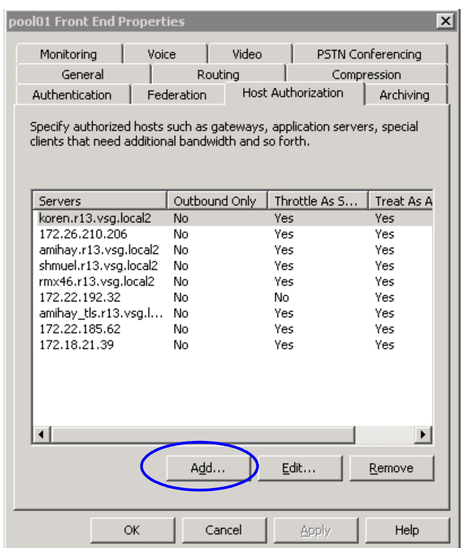


3 Right-click the *server pool* icon, click **Properties > Front End Properties**.

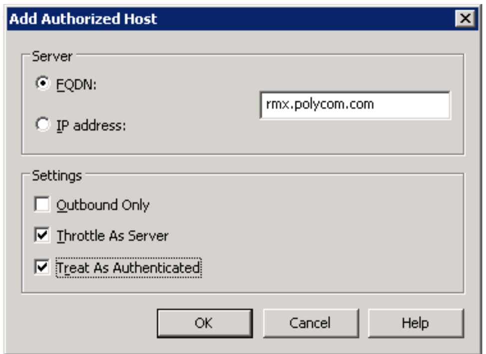


The *Pool Front End Properties* dialog box opens.

4 Click the **Host Authorization** tab.



5 Click the **Add** button to add the MCU as trusted host.
The *Add Authorized Host* dialog box opens.



6 In the *Add Authorized Host* dialog box, enter the MCU *FQDN* name as defined in the DNS and will be used in the Static Routes definition.

7 In the *Settings* section, select the **Throttle as Server** and **Treat As Authenticated** check boxes.

8 Click **OK**.
The defined MCU appears in the trusted servers list in the server *Front End Properties – Host Authorization* dialog box.

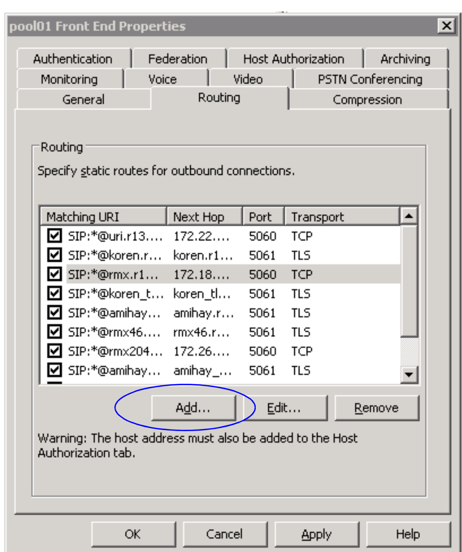
> If routing between the MCU and the OCS using Static Routes is required, do not close this dialog box, and continue with the following procedure. If you do not want to define Static Routes, click OK to close this dialog box.

Setting the Static Route for MCU in the OCS

To add MCU to the Routing Roles:

9 In the *Front End Properties* dialog box, click the **Routing** tab.

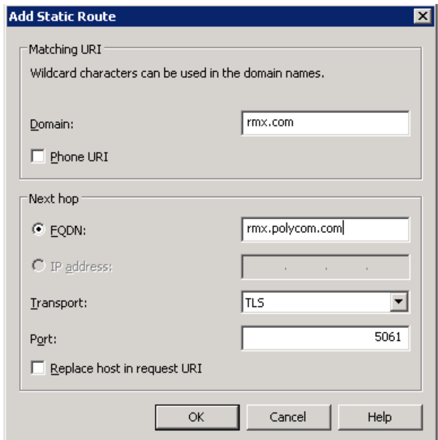
10 Click the **Add** button.



The *Add Static Routes* dialog box opens.

11 In the *Matching URI* section, enter the *Domain* name for the MCU. Any domain name can be used.

12 In the *Next hop* section enter the MCU *FQDN* name as defined in the DNS and is used in the *Host Authorization* definition.



13 In the *Transport* field, select **TLS** to enable the dial-out from conferences to SIP endpoints.

14 Click **OK**.
The new Route is added to the list of routes in the *Front End Properties – Routes* dialog box.

15 Click **OK**.

Optional. Setting the Static Route & Trusted Host for MCU in the Load Balancer Server

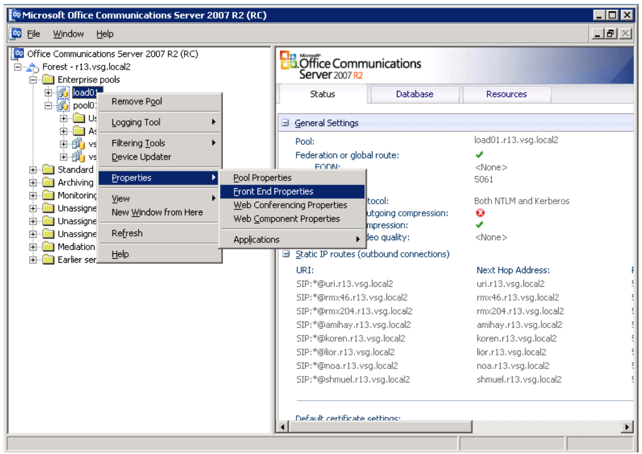
If your network includes a Load Balancer server, the MCU unit must be configured as a trusted host in the Load Balancer server in the same way it is configured in the OCS. In addition, Static Routes must also be defined in the Load Balancer server in the same way it is configured in the OCS, however, the Load Balancer should be pointed to the OCS pool and not to the MCU directly. This configuration procedure is done in addition to the configuration in the OCS.

To set the MCU as trusted and define Static routes in the Load Balancer Server:

1 Open the OCS Management application.

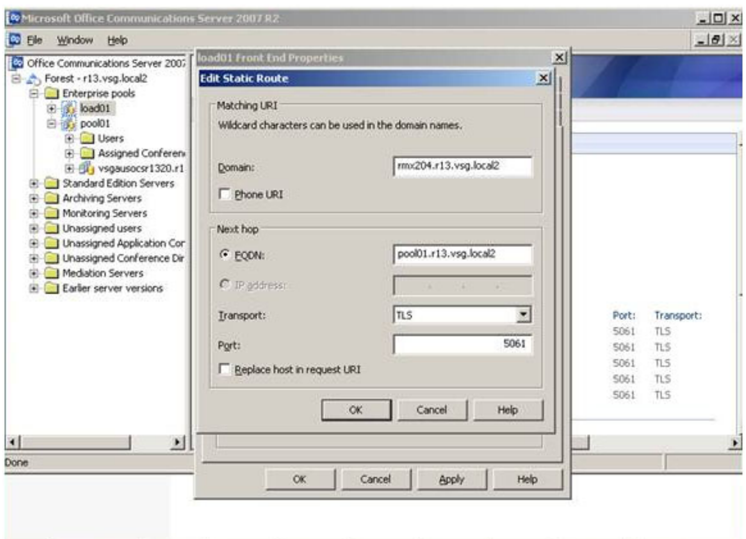
2 Expand the *Enterprise Pools* list.

3 Right-click the *Load* icon, click **Properties > Front End Properties**.



The *Load Front End Properties* dialog box opens.

The definition procedure is the same as for setting the MCU as trusted and define Static routes in the OCS. For details, see *"Setting the Trusted Host for MCU in the Office Communications Server"* on page 7.



Make sure that when defining the Static Route it is pointing to the OCS pool and not to the MCU directly.

Configuring the MCU System

The required tasks are detailed in "*Configuring the RMX 1500/2000/4000 for Microsoft Integration"* on page **H-36**.

Dialing to an Entry Queue, Meeting Room or Conference Using the Matched URI Method

Once the MCU is configured for integration in the OCS environment (for details, see "*Configuring the RMX 1500/2000/4000 for Microsoft Integration"* on page **H-36**), the preferred dialing mode to the conferencing entities such as Meeting Rooms, conferences and Entry Queues is direct dial in using the domain name defined in the OCS Static Routes. This eliminates the need to register the conferencing entities with the SIP server and to define a separate user for each conferencing entity in the Active Directory.

In such a case, after the first dial in, the conferencing entity will appear in the OC client directory for future use.

To dial in directly to a conference or Entry Queue:

Enter the conferencing entity SIP URI in the format:
conferencing entity routing name@domain name

The domain name is identical to the domain name defined in the OCS Static Routes.

For example, if the domain name defined in the OCS static routes is lcs2007.polycom.com and the Routing Name of the Meeting Room is 4567, the participant enters 4567@lcs2007.polycom.com.

Another dialing method is to register the Entry Queues with the SIP Server and create a user for each Entry Queue in the Active Directory. In such a case, OC clients can select the Entry Queue from the Contacts list and dial to the Entry Queue.

Setting the Numerical Dialing Method

The MCU can be configured as a Voice Gateway in the OCS environment, enabling dialing in to meeting rooms using numbers instead of or in addition to SIP URI addresses which are long strings.

In such configuration, HDX or MOC users dial a number rather than a full SIP URI, simplifying the dialing, which is especially beneficial with the HDX remote control.

Such configuration also enables a common dialing plan for meeting rooms across OCS and H.323 infrastructures. In an integrated environment that also includes Microsoft Exchange Server and Polycom Conferencing Add-in for Microsoft Outlook, a single number can be inserted into a calendar invitation and it will be valid for OC client endpoints and H.323 endpoints.

This dialing method can be configured in parallel to the matching URI dialing method (using Static Routes).

Setting the Numerical Dialing for MCU Meeting Rooms

The following processes are required to set up the numerical dialing for the MCU Meeting Rooms in the OCS infrastructure:

OCS side:

- Configuring the MCU as a Routable Gateway - The MCU (or DMA) must be set as a trusted voice gateway in the OCS infrastructure. This does not restrict MCU to just voice operation, rather it means that the MCU (or DMA) can be set as a destination for a voice route using the OCS management console.
  Setting the MCU as a trusted voice gateway also enables it to be used as a trusted gateway for static routes using URI matching.

- Establishing a Voice Route to the MCU "Voice" Gateway - The Voice Route to the MCU (or DMA) must be configured in the OCS infrastructure.

> If the MCU was previously defined as a Trusted Host for matching URI dialing method, this definition must be removed before configuring the MCU as a voice gateway. It will be defined as trusted host as part of the voice gateway configuration. For more details, see *Optional. Removing the MCU from the Host Authorization List*.

- Configure Office Communicator Users for Enterprise Voice.

MCU side:

The following tasks are detailed in "*Configuring the RMX 1500/2000/4000 for Microsoft Integration"* on page **H-36**.

1 Modify the Management Network Service to include the DNS server and set the Transport Type to TLS.

2 Create the security certificate (using one of the two available methods)

3 Define a SIP Network Service in the MCU and install the TLS certificate.

4 Modify and add the required system flags in the MCU System Configuration.

5 **Optional.** Defining additional Entry Queues and Meeting Rooms in the MCU environment. For details see "*Meeting Rooms"* on page **6-1** and "*Entry Queues"* on page **7-1**.

For a detailed description of the configuration of the Polycom conferencing components for the integration in Microsoft Office Communications Server 2007 see *Polycom® HDX and MCU™ Systems Integration with Microsoft Office Communications Server 2007 Deployment Guide.*

Optional. Removing the MCU from the Host Authorization List

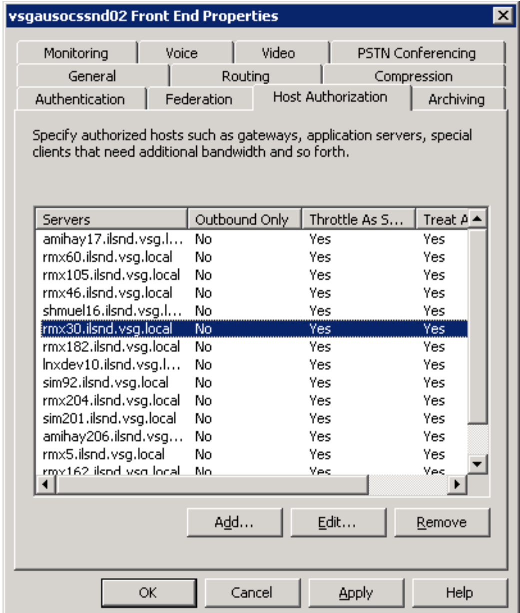
If you have defined the MCU as Trusted Host to enable dialing using the Static Routes and you want to use numerical dialing in addition or instead of SIP URI dialing, you need to remove the current definition of the MCU and redefine it as a voice gateway.

To remove the definition of the MCU as trusted host from the Front End Properties:

1 In the OCS application, display the *Front End Properties* (right-click the Front End and select Properties).

2 Click the **Host Authorization** tab.

3 In the *Trusted Hosts* list, click the MCU entry and then click the **Remove** button.



4 Click **OK**.

Configuring the MCU as a Routable Gateway

The MCU must be set as a routable voice gateway in the Office Communications Server infrastructure. This does not restrict the MCU to just voice operation, rather it means that the MCU can be set as a destination for a voice route in the Office Communications Server infrastructure.

The Office Communications Server infrastructure uses the WMI class `MSFT_SIPTrustedAddInServiceSetting` to store information for each voice gateway in the infrastructure. Typically, these gateways are Office Communications Server Mediation Servers, but in this case, the MCU is set as a voice gateway by creating a new instance of the class `MSFT_SIPTrustedAddInServiceSetting`.

Polycom recommends using the Office Communications Server 2007 R2 Resource Kit Tools to accomplish this.

To set up the MCU/DMA as a Voice Gateway:

1 Download and install the Office Communications Server 2007 R2 Resource Kit Tools from the following URL:

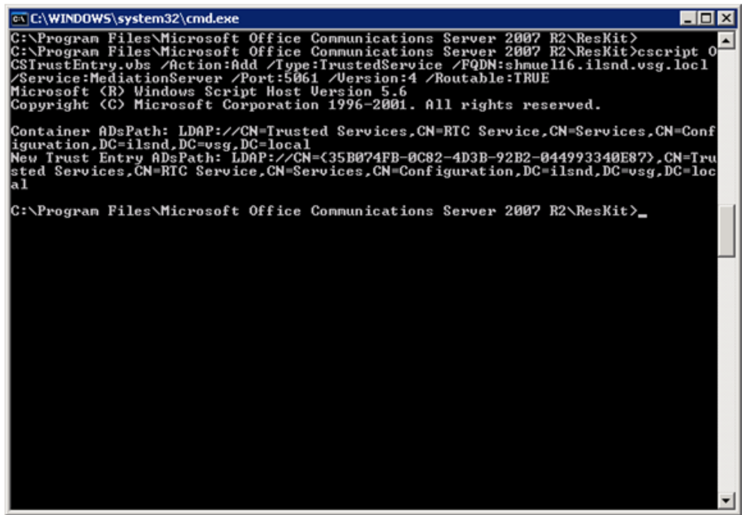
http://www.microsoft.com/downloads/details.aspx?familyid=9E79A236-C0DF-4A72-ABA6-9A9602A93ED0&displaylang=en

2 Open a command prompt and navigate to where you installed the resource kit. For example, `C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\`.

3 Run the following command:

`cscript OCSTrustEntry.vbs /action:add /type:trustedservice /fqdn:<your FQDN> /service:MediationServer /port:5061 /version:4 /routable:TRUE`

Where `<your FQDN>` is the FQDN of your MCU system. The script automatically generates the GUID discover the proper Active Directory container to store the object.



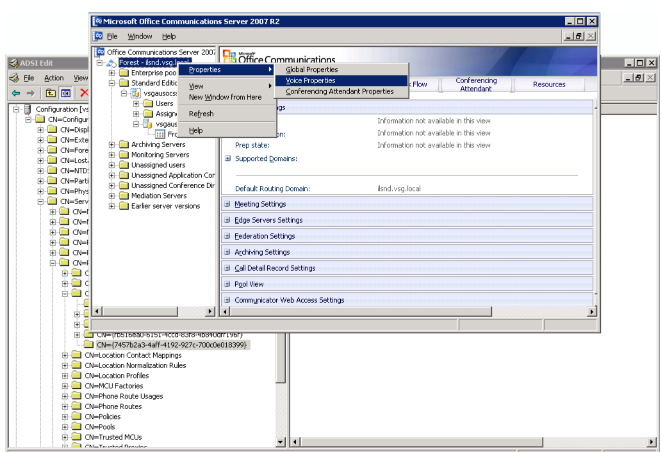
Your MCU system is now established as a trusted gateway by all Office Communications Server pools in the domain. It appears in the list of voice gateways when you establish a voice route.

Establishing a Voice Route to the MCU "Voice" Gateway

The OCS infrastructure enables you to establish a voice route to a voice gateway. Typically, this means that all SIP INVITEs to phone numbers which match a particular pattern will be routed to a specific gateway. In this example, all INVITEs to numbers which start with "11" will be routed to MCU11 (DNS name rmx11.r13.vsg.local2).

To establish the voice route:

1 Open the OCS R2 management Console and right click on **Forest** and then click **Properties > Voice Properties**.

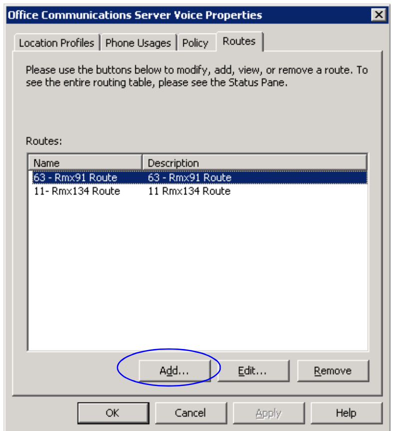


The *Office Communications Server Voice Properties* dialog box opens.

2 Click the **Routes** tab.

Office Communications Server Voice Properties - Routes dialog box opens.

3 Click the **Add** button.

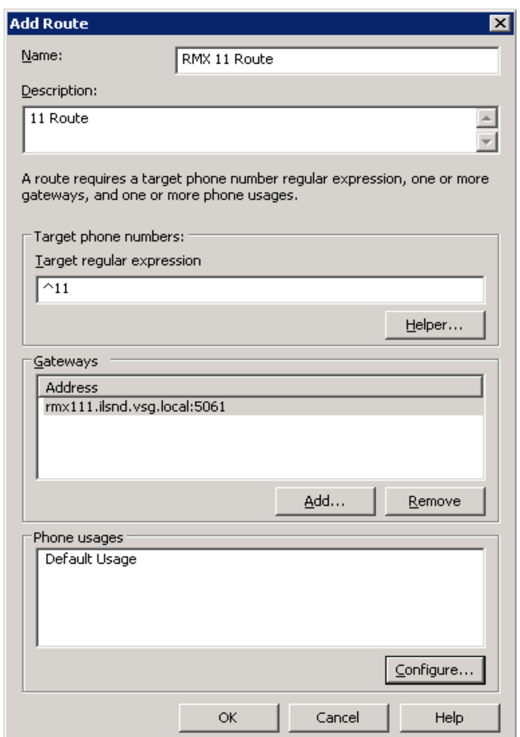


The *Add Route* dialog box opens.

4 In the *Name* field, enter a name that will identify this voice route.

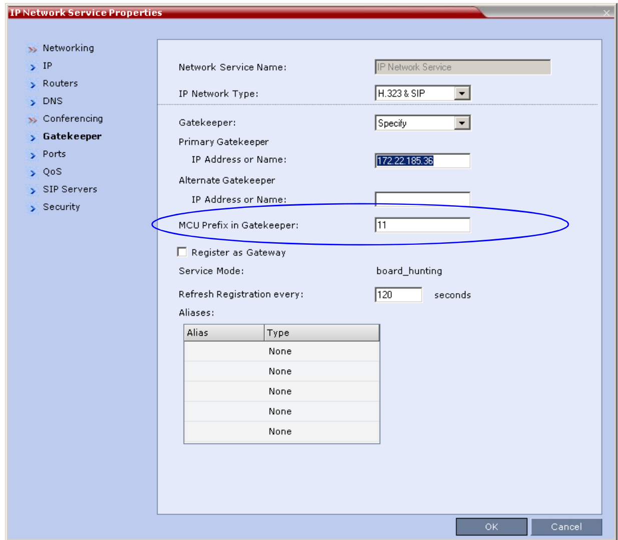
5 Optional. In the *Description* field, enter a description.

6 In the *Target Regular Expression* field enter **^** and the MCU prefix as defined in the gatekeeper. This prefix is also defined in the *MCU IP Network Service*.

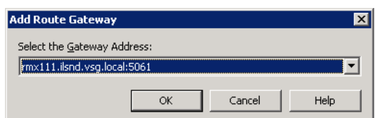


For example, if 11 is the MCU prefix defined in gatekeeper, enter **^11**. The circumflex expression "^11" causes this route to be applied to all numbers starting with "11".

If you have not defined such a prefix in the IP Network Service in the MCU configuration, you can add it later, using value entered here.



7 In the *Gateways - Addresses* box, click the **Add** button.
The *Add Route Gateway* dialog box opens.

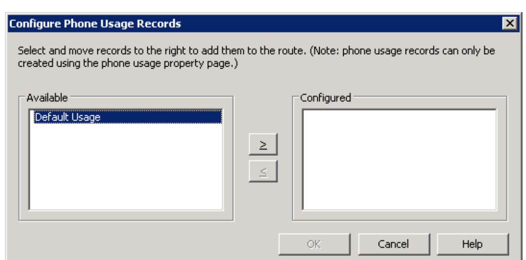


8 Select the MCU gateway address that was set up in *Configuring the MCU as a Routable Gateway* that appears in the drop down list of gateways.

9 Click **OK** to save the address and return to the *Add Route* dialog box.

10 In the *Phone Usage* box, click the **Configure** button.
The *Configure Phone Usage Records* dialog box opens.

11 In the *Available* box, click **Default Usage** and then click the **>** button.



The *Default Usage* option appears in the *Configured* box.

12 Click **OK**.

13 In the *Add Route* dialog box, click **OK** to save the new route.

Configuring Office Communicator Users for Enterprise Voice

Each of the endpoints in the OCS environment must be set to use the voice route.

The setting is done in the Office Communications Server management console for all required users (endpoints) simultaneously or in the Active Directory for each of the Users (endpoints).

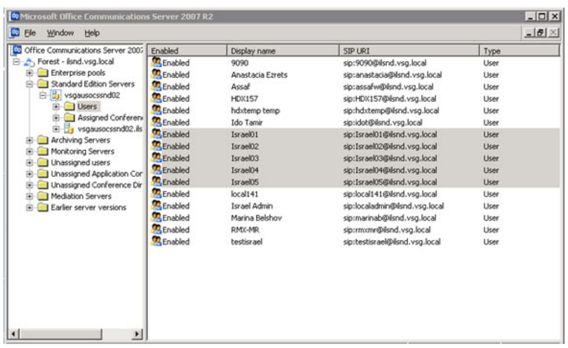
To Configure Office Communicator Users for Enterprise Voice in the Office Communications Server management console:

1 Navigate to **Start > All Programs > Administrative Tools > Office Communications Server 2007 R2** to open the Office Communications Server management console.

2 Expand the Enterprise pool or Standard Edition server node where your users reside.

3 Expand the pool or server where your users reside, and then click the **Users** node.

4 In the right pane, right-click one or more users whom you want to configure, and then select **Configure users**.



The *Welcome to the Configure Users Wizard* opens.

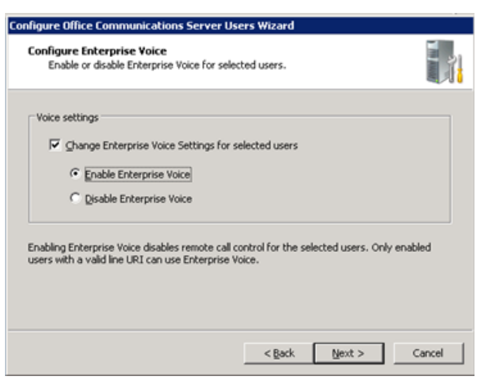
5 On the *Welcome to the Configure Users Wizard* dialog box, click **Next**.

6 On the *Configure User Settings* dialog box, click **Next**.

7 On the *Configure Meeting Settings* dialog box, click **Next**.

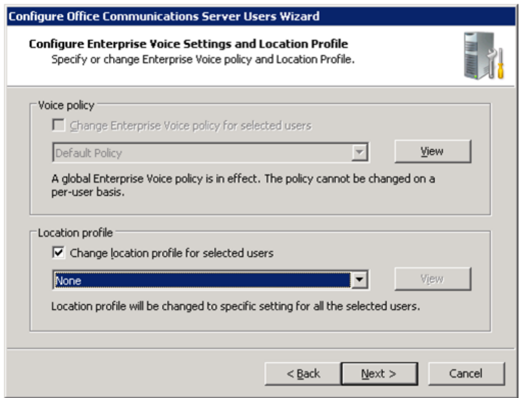
8 On the *Configure User Settings specify meeting policy* dialog box, click **Next**.

9 On the *Configure Enterprise Voice* dialog box, select **Change Enterprise Voice Settings for selected users**, and then click **Enable Enterprise Voice**. Click **Next**.



10 On the *Configure Enterprise Voice Settings and Location Profile* dialog box, select **Change Enterprise Voice Policy for selected users**.

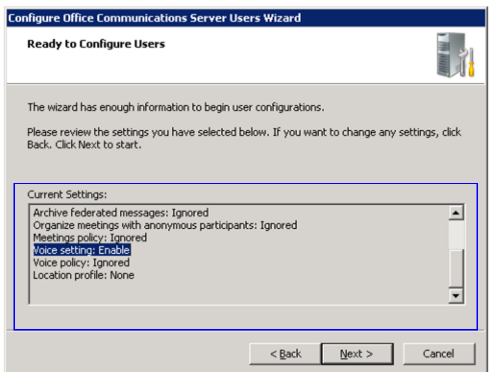
11 Select an Enterprise Voice policy from the list.



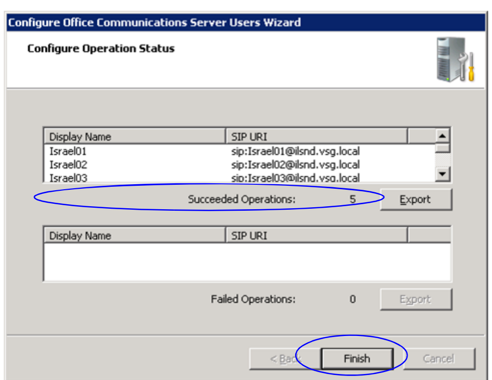
12 Select **Change location profile** for selected users.

13 Select a location profile from the list, and then click **Next**.

14 On the *Ready to Configure Users* dialog box, review the settings, and then click **Next**.



15 On the *Configure Operation Status* dialog box, verify that the operation succeeded, and then click **Finish**.

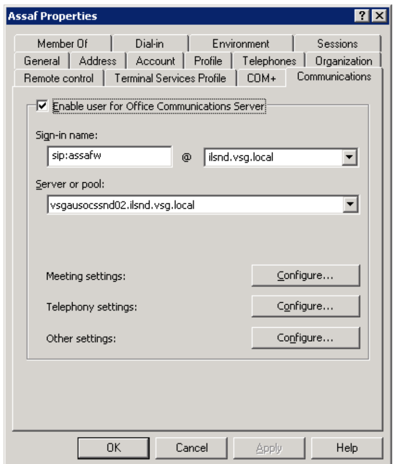


To Configure Office Communicator Users for Enterprise Voice in the in the Active Directory:

1 Open the *Active Directory* and navigate to the endpoint whose properties require changing.

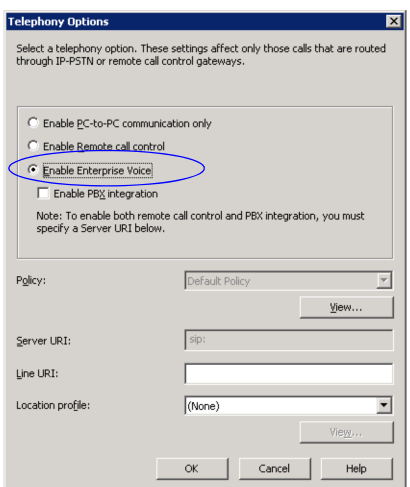
2 Right-click the endpoint and select **Properties**.
The *Properties* dialog box opens.

3 Click the **Communications** tab.



4 Click the **Telephony Settings** - **Configure** button.
The *Telephony Options* dialog box opens.

5 Select the **Enable Enterprise Voice** option.

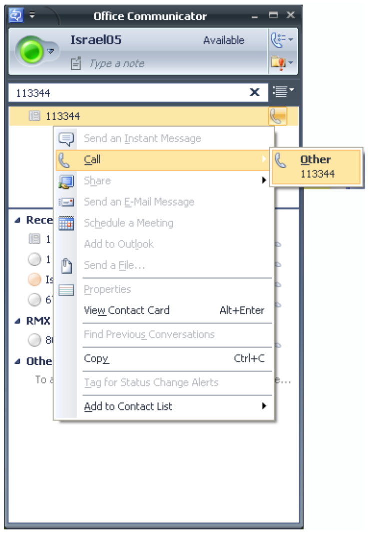


6 Click **OK** to return to the *Properties - Communications* dialog box**.**

7 Click **OK**.

Starting a Conferencing Call from the MOC

1 In the Office Communicator application, enter the number to dial, for example, 113344. This number is composed of the MCU Prefix in the Gatekeeper (for example, 11) and the Meeting Room ID, as defined on the MCU (for example, 3344).



2 Click **Call**, and then click **Other**.
The call is routed to the Meeting Room on the MCU, and the caller that initiated the call connects as the conference chairperson.

3 The MOC User can then add video to the call, by selecting **Add Video** in the *Office Communicator* window.

Setting Simultaneous Numerical Dialing and Matched URI Routing

You can simultaneously set up an MCU for both numerical and Matched URI dialing. If you want to do this, follow these instructions:

1 Set the MCU as a trusted service (MediationServer) and a voice gateway using the instructions in "*Setting the Numerical Dialing Method"* on page **H-12**.

2 Set up a matching URI route to the MCU/DMA by right-clicking the **OCS Pool**, selecting **Properties > Front End Properties > Routing Tab** and follow the instructions in "*Setting the Static Route for MCU in the OCS"* on page **H-9**.

- When defining both routing methods, you **cannot** add an MCU as an Authorized Host using the **Front End Properties > Host Authorization** tab. There can only be one trusted service entry for the MCU even though there are two different routes to the MCU (i.e., Matched URI and numerical dialing). If the Matched URI routing method was previously defined and the MCU was set as trusted host, and you are adding the numerical dialing method, you have to remove the MCU from the Trusted Hosts list. For more details, see "*Optional. Removing the MCU from the Host Authorization List"* on page **H-13**.
- Only TLS connections to the MCU will work, TCP connections will not work.

PFX Method - Creating the Security (TLS) Certificate in the OCS and Exporting the Certificate to the MCU Workstation

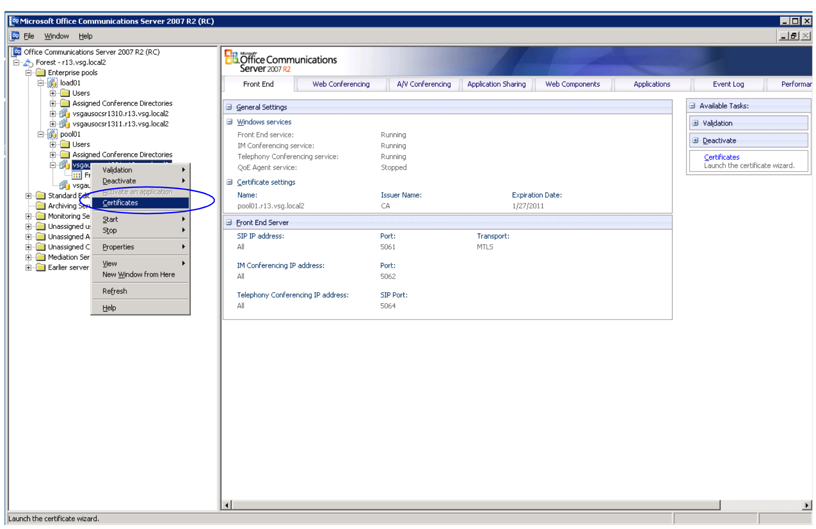
If you are using the PFX method to create and send the security certificate to the MCU, certificate files *rootCA.pem*, *pkey.pem* and *cert.pem* must be sent to the MCU unit. These files can be created and sent to the MCU in two methods:

- The files *rootCA.pem*, *pkey.pem* and *cert.pem* are provided by a Certificate Authority and are sent independently or together with a password file to the MCU. This is the recommended method.
- Alternatively, the TLS certificate files are created internally in the OCS and exported to the MCU workstation from where the files can be downloaded to the MCU. If the certificate is created internally by the OCS, one **.pfx* file is created. In addition, a text file containing the password that was used during the creation of the **.pfx* file is manually created. Both files can then be sent from the MCU workstation to the MCU unit. When the files are sent to the MCU, the **.pfx* file is converted into three certificate files: *rootCA.pem*, *pkey.pem* and *cert.pem*.
  Sometimes, the system fails to read the *.pfx file and the conversion process fails. Resending *.pfx file again and then resetting the system may resolve the problem.

The following procedure describes how to create the *.PFX file in the OCS and export it so it can be sent to the Certificate Authority or to the MCU.

To create the TLS certificate in the Office Communications Server:

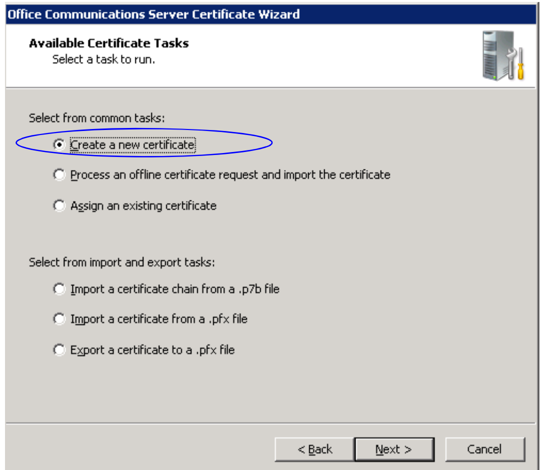
1. In the OCS *Enterprise Pools* tree, expand the Pools list and the *server pool* list.
2. Right-click the pool *Front End* entity, and click **Certificate**.



The *Office Communicator Server Wizard Welcome* window is displayed.

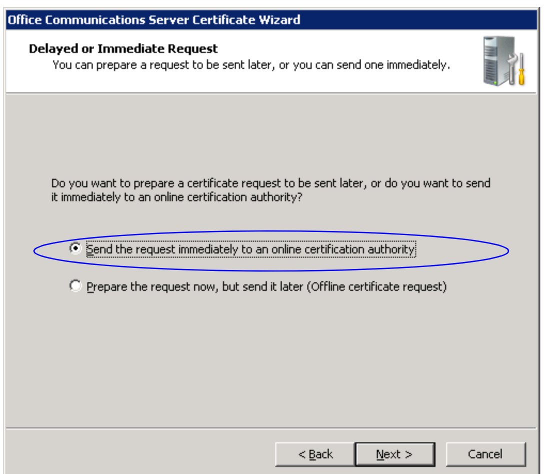
3. Click **Next**.
   The *Available Certificate Tasks* window appears.

4 Select **Create a New Certificate** and click **Next**.



The *Delayed or Immediate Request* window appears.

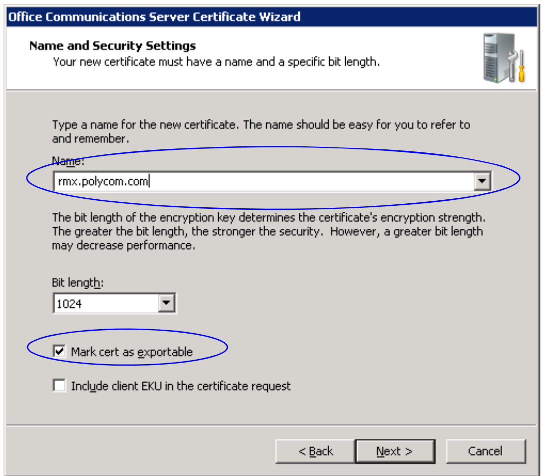
5 Select **Send the Request immediately to an online certificate authority** and click **Next**.



The *Name and Security Settings* window appears.

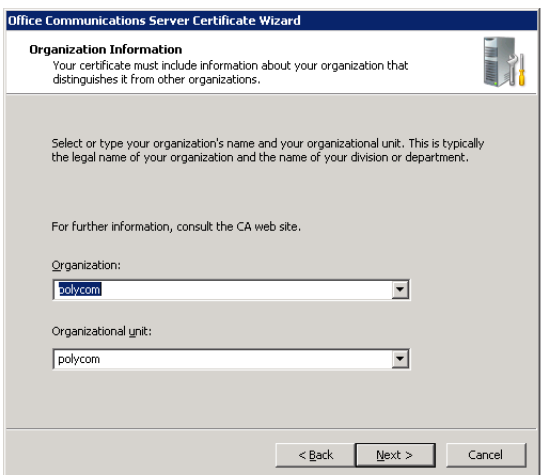
6 In the *Name* field, select the MCU name you entered in the *FQDN* field when defining the trusted host or as defined in the DNS server.

7 Select the **Mark cert as exportable** check box.



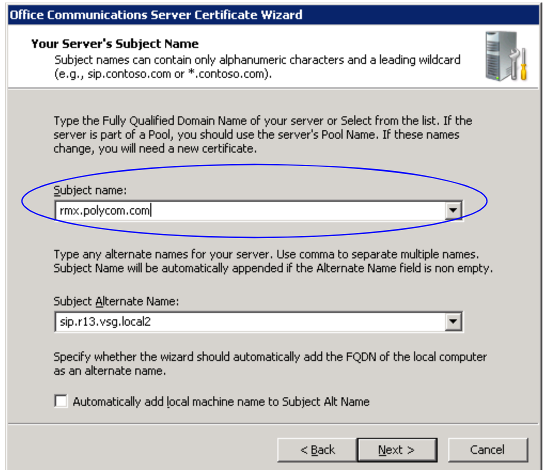
8 Click **Next**.
The *Organization Information* window appears.

9 Enter the name of the *Organization* and the *Organization Unit* and click **Next**.



Your Server's Subject Name window appears.

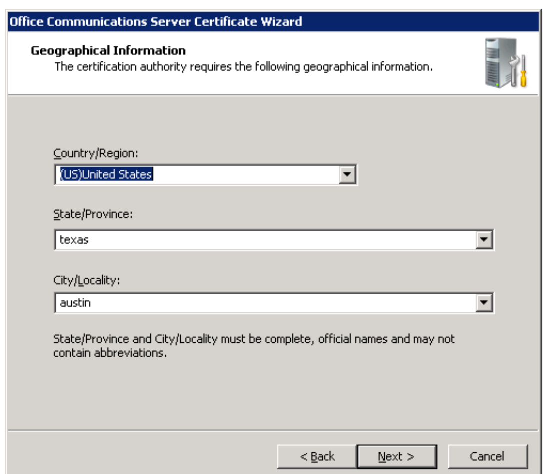
10 In the *Subject name* field, select the *FQDN* name of the MCU from the list or enter its name.
Keep the default selection in the *Subject alternate name* field and click **Next**.



11 If an error message is displayed, click **Yes** to continue.

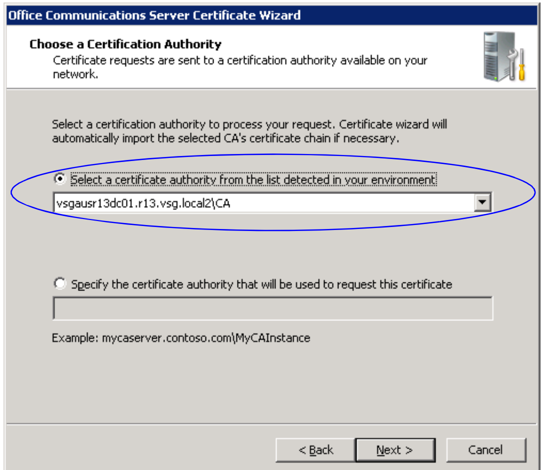
The *Geographical Information* window appears.

12 Enter the geographical information as required and click **Next**.



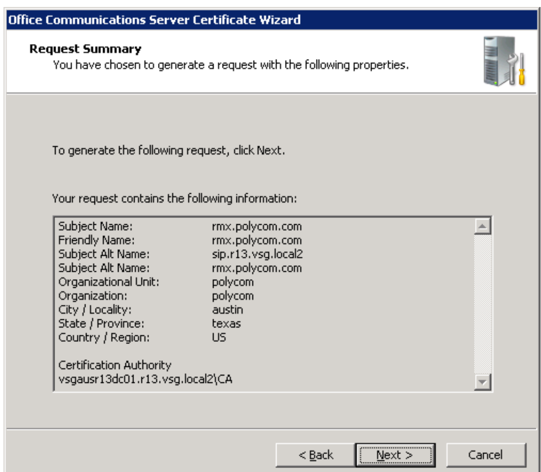
The *Choose a Certification Authority* window appears.

13 Ensure that the **Select a certificate authority from the list detected in your environment** option is selected and that the local OCS front end entity is selected.



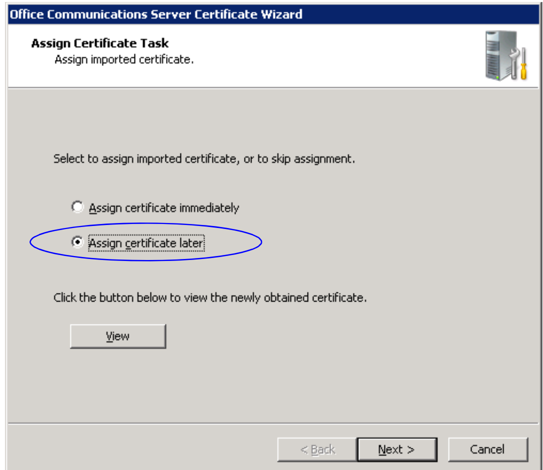
14 Click **Next**.
The *Request Summary* window appears.

15 Click **Next** to confirm the listed parameters and create the requested certificate.



The *Assign Certificate Task* window appears.

16 Select **Assign certificate later** and click **Next** (MS R2).



The *Certificate Wizard Completed* window appears (MS R2).

17 Click **Finish** (MS R2).

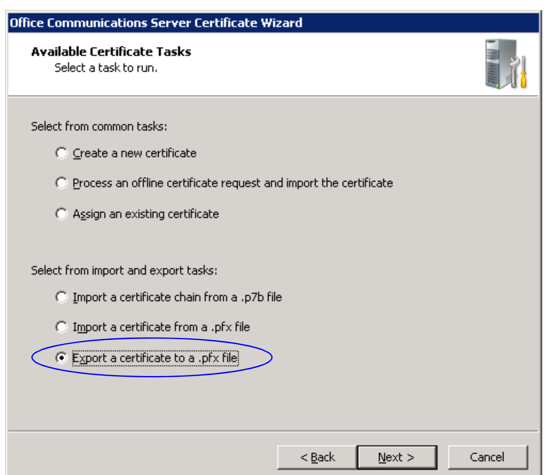
Retrieving the Certificate from the OCS to be sent to the MCU Workstation

1 In the OCS *Enterprise Pools* tree, expand the *Pools* list and the *Server Pool* list.

2 Right-click the *pool Front End* entity, and select **Certificate**.

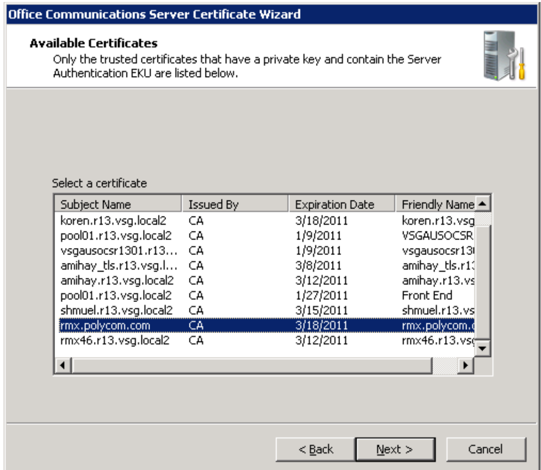
The *Available Certificate Tasks* window appears.

3 Select **Export a certificate to a *.pfx file** and click **Next**.



The *Available Certificates* window appears.

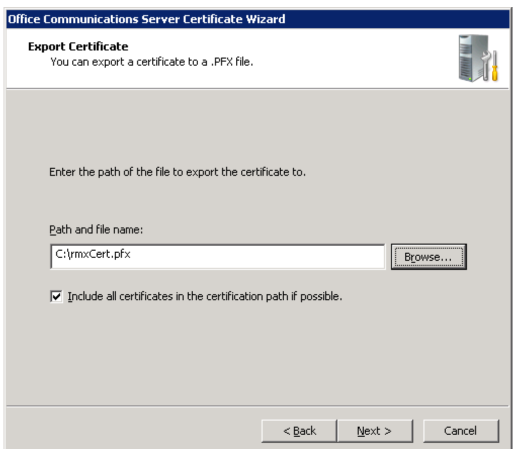
4 Select the certificate *Subject Name* of the MCU and click **Next.**



The *Export Certificate* window appears.

5 Enter the path and file name of the certificate file to be exported or click the **Browse** button to select the path from the list.

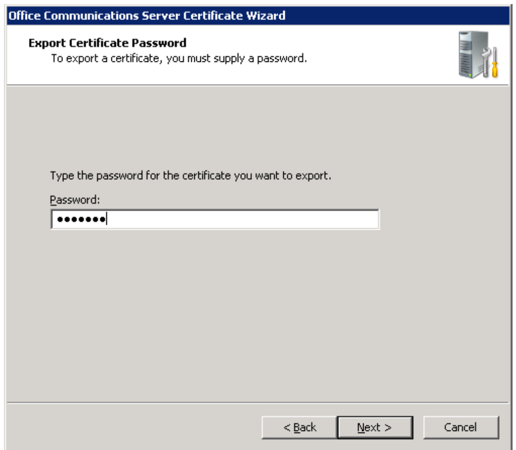
The new file type must be ***.pfx** and its name must include the **.pfx** extension.



6 Select the **Include all certificates in the certification path if possible** check box and then click **Next**.

The *Export Certificate Password* window appears.

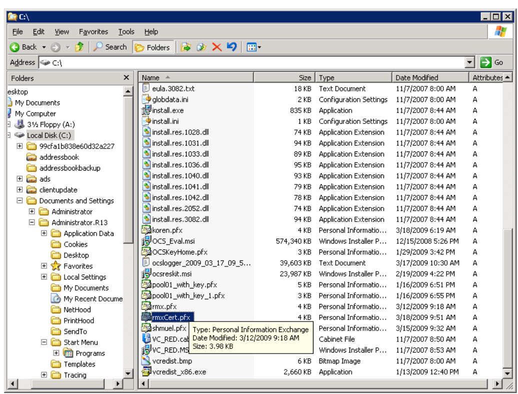
7 If required, enter any password. For example, *Polycom*.
Write down this password as you will have to manually create a password file in which this password will appear.



Click **Next**.
The *Certificate Wizard Completed* window appears.

8 Click **Finish**.

The created *.*pfx* file is added in the selected folder.



Optional. Creating the Certificate Password File (certPassword.txt)

If you have used a password when creating the certificate file (*.*pfx*), you must create a **certPassword.txt** file. This file will be sent to the MCU together with the *.*pfx* file.

To create the certPassword.txt file:

1 Using a text editor application, create a new file.

2 Type the password as you have entered when creating the certificate file. For example, enter *Polycom*.

3 Save the file naming it **certPassword.txt** (file name must be exactly as show, the MCU is case sensitive).

Supporting Remote and Federated Users in Office Communications Server ICE Environment

To enable the remote and Federation connections the following operations must be performed:

- Create an Active Directory account for the MCU that will be used for registering and operating in the MS ICE environment
- Enable the MCU User Account for Office Communication Server
- Configure the MCU for ICE dialing for more details, see "*Configuring the MCU for Federated (ICE) Dialing"* on page **H-63**.

To place federated calls between Domain A and Domain B in ICE environment sub domains must be federated to the main domain or the MCU system must be installed on a main domain.

The MCU can also be set for Matched URI Routing and/or Numerical Dialing to Meeting Rooms. For more details, see "*Setting the Matched URI Dialing Method"* on page **H-6** and "*Setting the Numerical Dialing Method"* on page **H-12**.

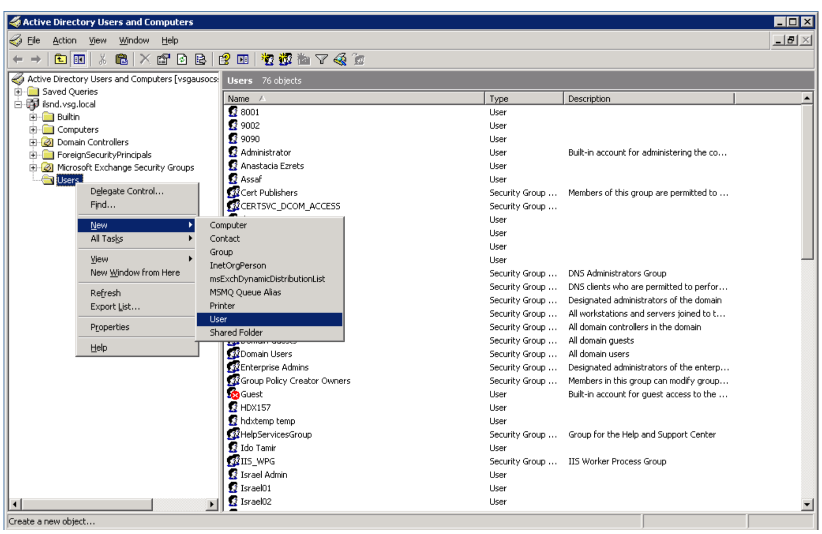
Creating an Active Directory Account for the MCU

The User account created for the MCU is used for registration in the Office Communication Server and to automatically synchronize with the STUN and relay (Edge) servers.

To add the MCU user to the Active Directory:

1 Go to **Start > Run** and enter **dsa.msc** to open the *Active Directory Users and Computers* console

2 In the console tree, select **Users > New > User**.



3 In the *New User* wizard, define the following parameters:

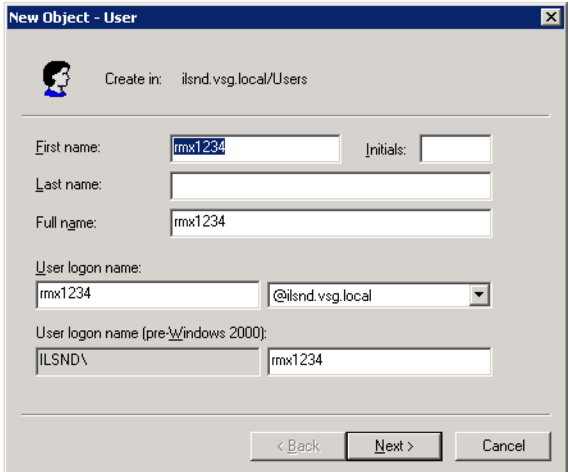
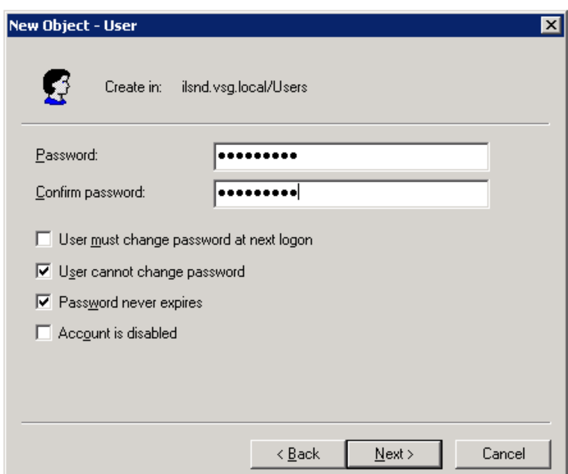


Table H-4 *Active Directory - New User Parameters for the MCU*

Field	Description
First Name	Enter the name for the MCU user. This name will be used in the configuration of the ICE environment in the MCU.
Full Name	Enter the same name as entered in the *First Name* field.
User Login Name	Enter the same name as entered in the *First Name* field and select from the drop down list the domain name for this user. It is the domain name defined for the Office Communication Server.

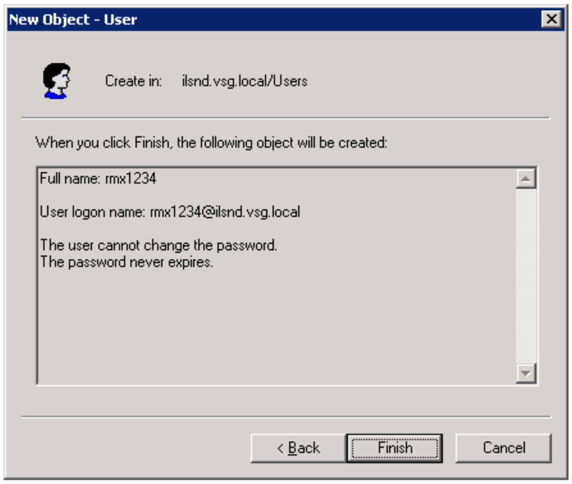
4 Click **Next**.

5 Enter the password that complies with the Active Directory conventions and confirm the password.



6 Select the options: **User cannot change password** and **Password never expires**. Clear the other options.

7 Click **Next**.
The system displays summary information.



8 Click **Finish**.

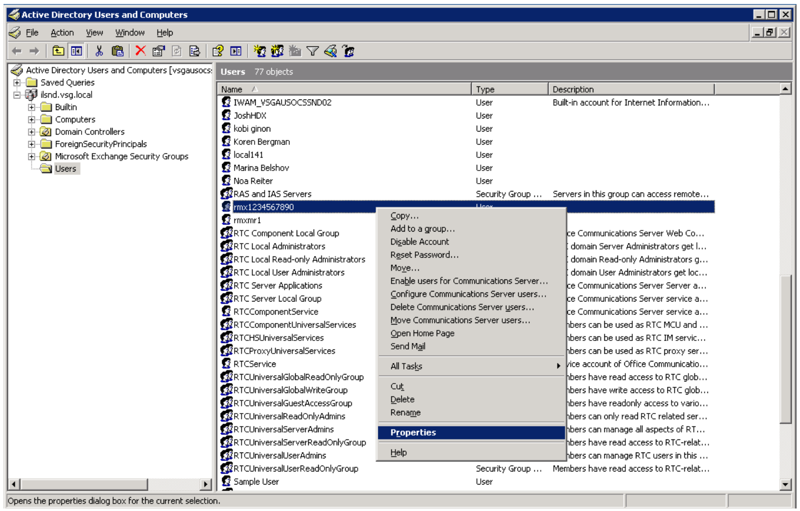
The new User is added to the Active Directory *Users* list.

Enabling the MCU User Account for Office Communication Server

The new MCU user must be enabled for registration with the Office Communications Server.

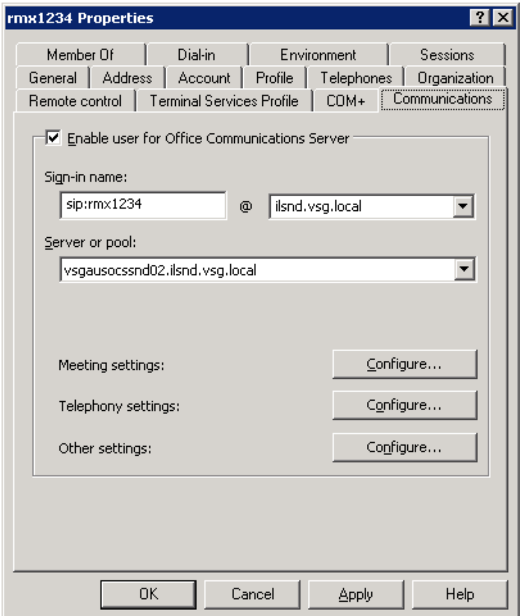
To enable the MCU User Account for Office Communication Server:

1 In the *Active Directory Users and Computers* window, right-click the MCU user and then click **Properties**.



2 In the *Properties* dialog box, click the **Communications** tab.

3 In the *Sign in name* field, enter the MCU user name in the format **SIP:rmx user name** (for example sip:rmx1234) and select the domain name (for example, ilsnd.vsg.local) as entered in the *New User* dialog box.



4 Select the *Server or Pool* from the list.

5 Click **Apply** and then **OK**.

Configure the MCU for ICE dialing

For details, see "*Configuring the MCU for Federated (ICE) Dialing"* on page **H-63**.

MCU Integration into the Microsoft Lync Server 2010 and Lync Server 2013 Environments

From Version 7.8, the RMX interoperability level with Lync 2013 is identical to Lync 2010. Lync 2013 is backward compatible with all RMX Lync 2010 features.

From Version 7.1, MCU systems can be integrated into the Microsoft Lync Server 2010 (Wave 14) environment.

In the Lync Server 2010 environment, only the Matched URI dialing (using the SIP URI address) is available as the call routing method.

Non-Lync endpoints connected to the same AVC-based conference as Lync endpoints running on the RMX, cannot participate in the desktop sharing session initiated by Lync participants.

Configuring the Polycom-Microsoft Solution

See the *Polycom Unified Communications Deployment Guide for Microsoft Environments*, *"Deployment Process for Polycom MCU Systems"* for detailed steps on how to deploy a Polycom MCU system for use with the video conferencing solution in Microsoft Lync Server 2010 environment.

Call Admission Control (CAC)

Microsoft Call Admission Control (CAC), a protocol that enables bandwidth management via the Policy Server in federated (ICE) environment, is supported on the MCU.

The Policy server functionality enables the Lync server to manage the bandwidth allocated to the Lync client when connecting to another Lync client or a video conference running on the MCU. The bandwidth allocated by the Policy server may be the same or lower than the bandwidth requested by the Lync client, which is based on the line rate of the conference.

Guidelines

- Microsoft CAC is available only with:
  - A Lync server (Wave 14)
  - Call Policy functionality enabled
  - The Call Admission Control enabled for the Lync Clients
  - ICE environment
  - Local network
  - MCU MPM+ and MPMx Card Configuration Modes
- Microsoft CAC is applicable only to dial-in calls
- Additional configuration on the Microsoft side is not required. It is based on the existing ICE environment configuration.
- Additional configuration (setting a system flag) may be required on the MCU to modify the system behavior when CAC is enabled in a local network; closing the ICE channel or keeping it open.
- Setting an additional system flag may be required on the MCU when running Video Switching conferences.

For more details, see "*MCU Configuration for CAC Implementation"* on page **H-60**.

FEC Support

Microsoft RTV FEC (Forward Error Correction) is supported in the MCU to control and correct packet loss when receiving and sending video streams using the Microsoft Lync Server 2010 communications software. All RTV resolutions and options, including B Frame, are supported.

Redundant video packets are sent over the network during video stream transmission. When packet loss occurs, FEC is automatically activated and the redundant packet is used to recover the lost packet.

When receiving video transmissions, packet loss automatically triggers FEC in the MCU. When sending video transmissions, MCU sends FEC packets when the RTCP RX report contains packet loss that is greater than or equal to 1 percent.

Media Over TCP

In previous MCU versions, media such as video, audio, content and FECC is transmitted using the UDP transport protocol. In version 7.7, media is automatically transmitted through TCP when UDP, the default transport protocol, is not available. Media over TCP is supported using the Microsoft ICE environment.

The media transport protocol type (UDP/TCP) is displayed in the *Participant Properties - Channel Status - Advanced* dialog box.

The media transport protocol type is displayed for the following IP addresses:

- MCU IP Address
- Participant IP Address
- ICE MCU IP Address - only when ICE is functional
- ICE Participant IP Address - only when ICE is functional

Network Error Recovery

When a short network error occurs, for example 5 seconds, MCU automatically recovers, enabling calls in Microsoft Lync to continue the video or audio conference without disconnecting. However, when a longer network error occurs, the call is disconnected. The presence status mode is correctly updated from *Busy* to *Available*. There is no configuration required for this procedure.

SIP Dialog Recovery

MCU has the ability to automatically recover from a SIP dialog failure, which can occur in long duration calls in Meeting Rooms using the Microsoft Lync client. There is no configuration required for this procedure.

Configuring the RMX 1500/2000/4000 for Microsoft Integration

The MCU is integrated in Microsoft Office Communications Server R2 (Wave 13) and Microsoft Lync Server environments by setting its *Transport Type* (in the SIP server configuration) to **TLS** and creating a certificate that is sent to the MCU. This procedure is also required when encryption of SIP signaling is used.

From Version 7.0.x, Microsoft R1 is not supported with MCU systems.

In addition, if the DNS server was not enabled in the *Network Management Service* on the MCU, it must be enabled for the integration in Microsoft Office Communications Server (R2, Wave 13) and the Lync Server (Wave 14) environments.

Modify the MCU Management Network Service to Include the DNS Server

The *Management Network* that is defined during first entry setup does not include the definition of the DNS which is mandatory in Microsoft environment and has to be modified.

In *Multiple Networks* configurations, A *DNS* server can be specified for each *IP Network Service* and for the *RMX Management Network Service*.

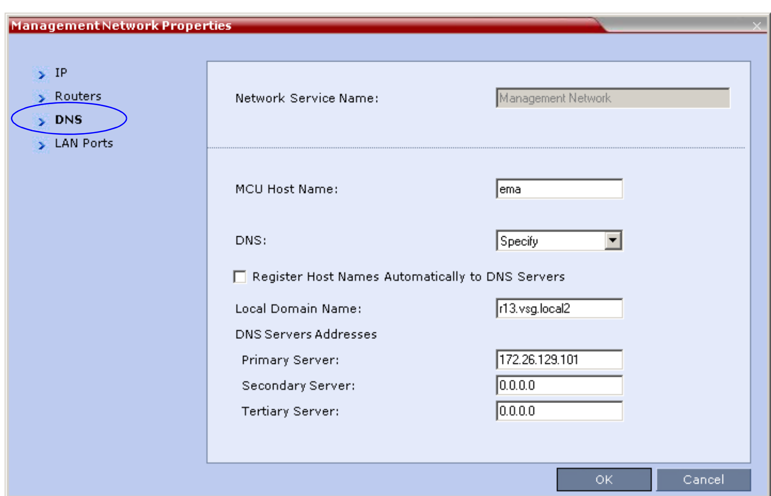
To add the definition of the DNS to the Management Network in the MCU:

1 Using the Web browser, connect to the MCU.

2 In the *MCU Management* pane, expand the **Rarely Used** list and click **IP Network Services** ( ).

3 In the *IP Network Services* pane, double-click the **Management Service** .
The *Management Network Properties - IP* dialog box opens.

4 Click the **DNS** tab.



5 In the *DNS* field, select **Specify** to define the DNS parameters.

6 View or modify the following fields:

Table 9 *Management Network Properties – DNS Parameters*

Field	Description
MCU Host Name	Enter the name of the MCU on the network. This name must be identical to the FQDN name defined for the MCU in the OCS and DNS. Default name is MCU.
Shelf Management Host Name	Displays the name of the entity that manages the MCU hardware. The name is derived from the MCU host name. Default is RMX_SHM.
DNS	Select: • **Off** – if DNS servers are not used in the network. • **Specify** – to enter the IP addresses of the DNS servers. **Note:** The IP address fields are enabled only if **Specify** is selected.
Register Host Names Automatically to DNS Servers	Select this option to automatically register the MCU Signaling Host and Shelf Management with the DNS server.
Local Domain Name	Enter the name of the domain where the MCU is installed as defined in the Office Communications Server/Lync Server.
DNS Servers Addresses:	
Primary Server	The static IP addresses of the DNS servers (the same servers defined in the Office Communications Server/Lync Server). A maximum of three servers can be defined.
Secondary Server	
Tertiary Server	

7 Click **OK**.

Defining a SIP Network Service in the MCU and Installing the Security Certificate

Your RMX 1500/2000/4000 system should be installed according to standard installation procedures. For details, see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide.

When configuring the *Default IP Network Service* on first entry, or when modifying the properties of the existing *Default IP Network Service*, the SIP environment parameters must be set as described in this section.

The Security Certificate

There are two methods to create and send the security certificate that is required for configuration of the integration of the MCU in the Microsoft environment:

- The CSR method (recommended method for Microsoft Office Communications Server, Wave 13)
- The PFX method (Recommended method for Lync Server, Wave 14)

The CSR Method

In the CSR method, the security certificate is created as part of the *SIP Server* configuration in the IP Network Service configuration.

Using the CSR Method, the following processes are performed:

- Creating the certificate request (in the *Default IP Network Service - SIP Server* dialog box).
- Sending the certificate request to a Certificate Authority.
- Receiving the certificate from the Certificate Authority.
- Installing the certificate in the MCU (in the *Default IP Network Service - SIP Server* dialog box).

The PFX Method

In the PFX method, the security certificate is created in advance, in the Office Communications Server or Lync Server environment.

For detailed description of this procedure in the Office Communications Server environment, see "*PFX Method - Creating the Security (TLS) Certificate in the OCS and Exporting the Certificate to the MCU Workstation"* on page **H-22**.

For detailed description of this procedure in the Lync Server environment, see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*..

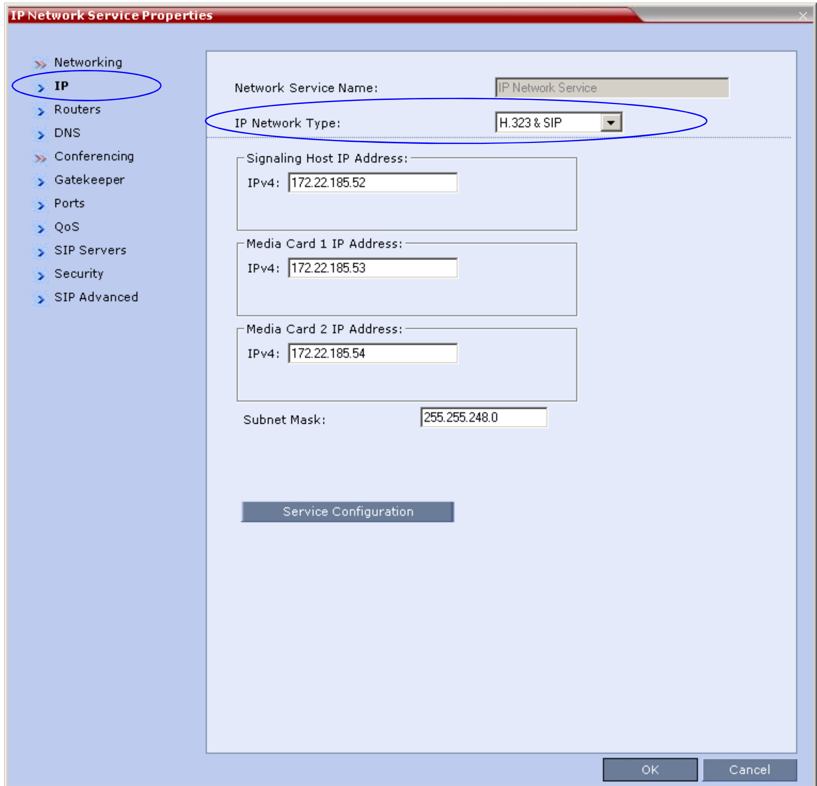
> Certificates are deleted when an administrator performs a *Restore Factory Defaults* with the *Comprehensive Restore* option selected.

Configuring the MCU IP Network Service

To configure the MCU IP Network Service:

1. Using the Web browser, connect to the MCU.
2. In the *MCU Management* pane, expand the **Rarely Used** list and click **IP Network Services** ( ).
3. In the *IP Network Services* pane, double-click the **Default IP Service** (, , or) entry.

The *Default IP Service - Networking IP* dialog box opens.

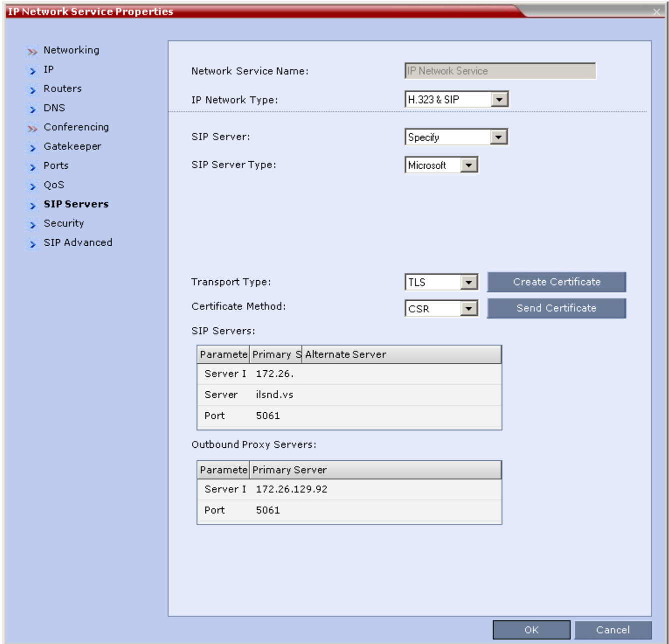


4 Make sure the *IP Network Type* is set to **H.323 & SIP** even though SIP will be the only call setup used with Office Communications Server 2007.

5 Make sure that the correct parameters are defined for the *Signaling Host IP Address, Media Card 1 IP Address, Media Card 2 IP Address* (RMX 2000/4000 if necessary), *Media Card 3 IP Address* (RealPresence Collaboration Server (RMX) 4000 if necessary), *Media Card 4 IP Address* (RealPresence Collaboration Server (RMX) 4000 if necessary) and *Subnet Mask*.

> Make sure that the IP address of the MCU Signaling Host is the same one defined as a trusted host in Office Communications Server 2007/Lync Server 2010.

6 Click the **SIP Servers** tab.



7 In the *SIP Server,* select **Specify.**

8 In the *SIP Server Type,* select **Microsoft**.

9 Enter the IP address of the Office Communications Server 2007 or Lync Server 2010 and the *Server Domain Name* as defined in the OCS/Lync Server and in the *Management Network* for the DNS.

10 If not selected by default, change the *Transport Type* to **TLS**.
The *Create Certificate* and *Send Certificate* buttons are enabled.

11 If you are using the CSR method, and the **CSR** option is not selected by default, change the *Certificate Method* to **CSR**.

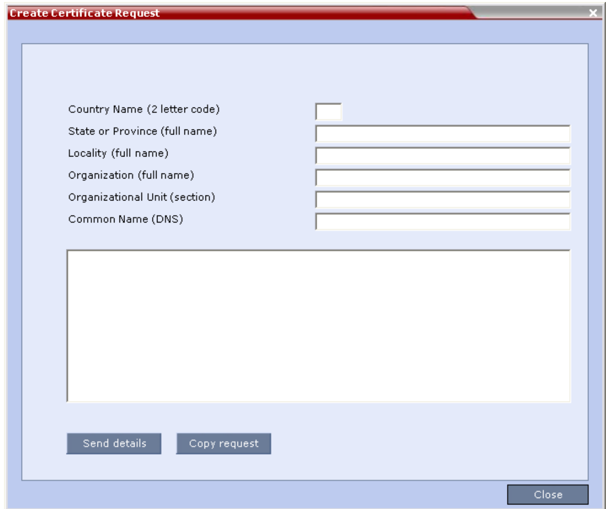
If you are using the PFX method, in the *Certificate Method* field select **PEM/PFX**.
At this point the procedure changes according to the selected certificate method.

If you have selected PEM/PFX, skip to step **27** on **page H-44.**

CSR Method - Creating the Certificate

12 Click the **Create Certificate** button.

The *Create Certificate Request* dialog box is displayed.



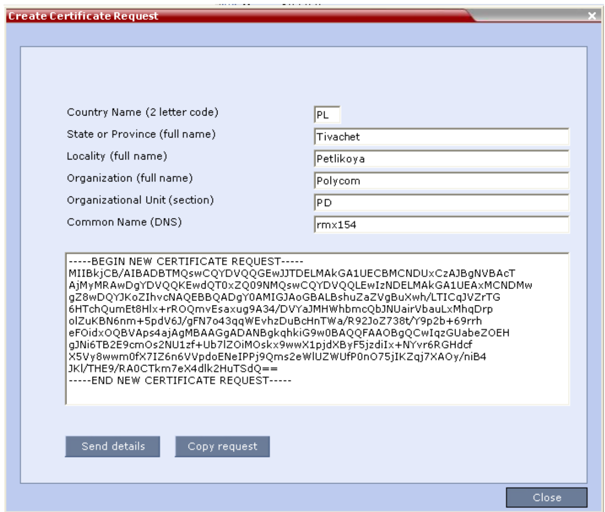
13 Enter information in all the following fields:

Table H-1 *Create Certificate Request*

Field	Description
Country Name	Enter any 2 letter code for the country name.
State or Province	Enter the full name of the state or province.
Locality	Enter the full name of the town/city/location.
Organization	Enter the full name of your organization for which the certificate will be issued.
Organizational Unit	Enter the full name of the unit (group or division) for which the certificate will be issued.
Common Name (DNS/ IP)	Enter the *DNS MCU Host Name*. This *MCU Host Name* must also be configured in the *Management Network Properties* dialog box.

14 Click **Send Details**.

The MCU creates a *New Certificate Request* and returns it to the *Create Certificate Request* dialog box along with the information the user submitted.



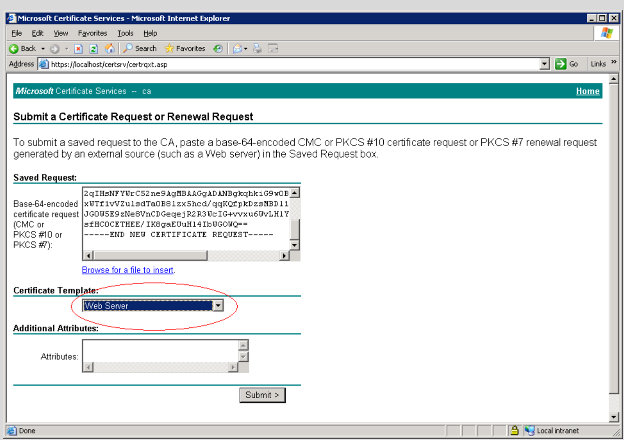
15 Click **Copy Request** to copy the *New Certificate Request* to the workstation’s clipboard.

16 Connect to your preferred *Certificate Authority’s* website using the web browser.

17 Follow the purchasing instructions at the *Certificate Authority’s* website.

18 Paste (**Ctrl + V)** the *New Certificate Request* as required by the *Certificate Authority*.

When creating the certificate request in the Certificate Authority site, make sure that the **Web Server** option is selected as the Certificate Template, as shown in the example below.



The *Certificate Authority* issues the TLS/SSL certificate, and sends the certificate to you by e-mail.

If the process of purchasing the certificate is short, you may leave the *IP Network Service - SIP Servers* dialog box open. Otherwise, close it without saving the changes to the Transport Type and Certificate Method.

CSR Method - Sending the certificate

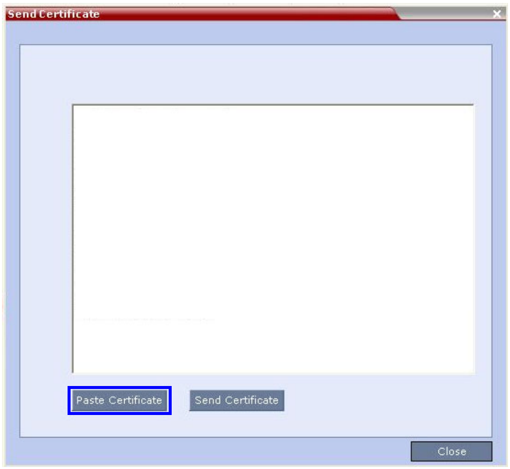
After you have received the certificate from the *Certificate Authority:*

> If you have closed the *IP Network Service - SIP Servers* dialog box, repeat steps 1 to 11 in the procedure "*Defining a SIP Network Service in the MCU and Installing the Security Certificate"* on page **H-37**.

19 Open the *Certificate Authority* e-mail and **Copy** (**Ctrl + C**) the certificate information from the *Certificate Authority's* e-mail to the clipboard.

20 In the *IP Network Service - SIP Servers* dialog box, click the **Send Certificate** button. The *Send Certificate* dialog box opens.

21 Click **Paste Certificate** to paste the clipboard content into the *Send Certificate* dialog box.



22 Click the **Send Certificate** button to send the certificate to the MCU.

23 Click the **Close** button.

24 In the *IP Network Service - SIP Servers* dialog box, complete the SIP Servers definitions.

25 Click **OK**.

The MCU validates the certificate.

— If the certificate is not valid, an error message is displayed.

— If the certificate matches the private key, and the task is completed, a confirmation message indicating that the certificate was created successfully is displayed.

Once the certificate is installed in the MCU you can complete the definition procedure or continue with the MCU configuration for ICE dialing. For details, see "*Configuring the MCU for Federated (ICE) Dialing”* on page **H-63**.

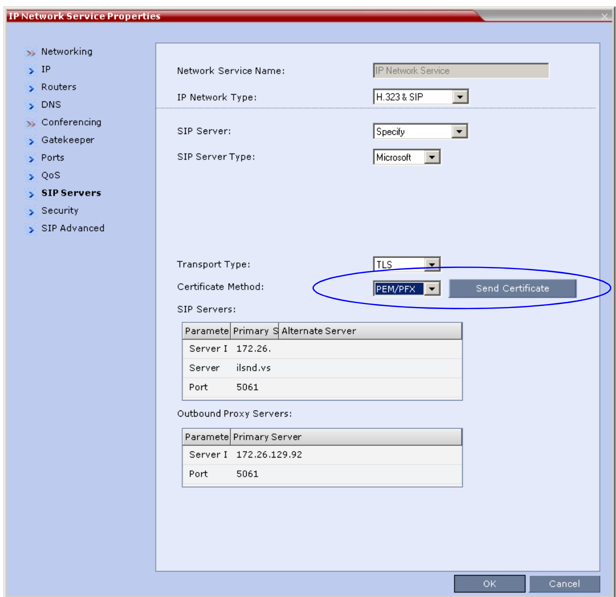
26 If no additional configuration is required, reset the MCU.

Reset can be performed after setting the system flags (for example, setting the MS_ENVIRONMENT flag). After system reset the MCU can register to the OCS server and make SIP calls.

PFX Method - Sending the Certificate

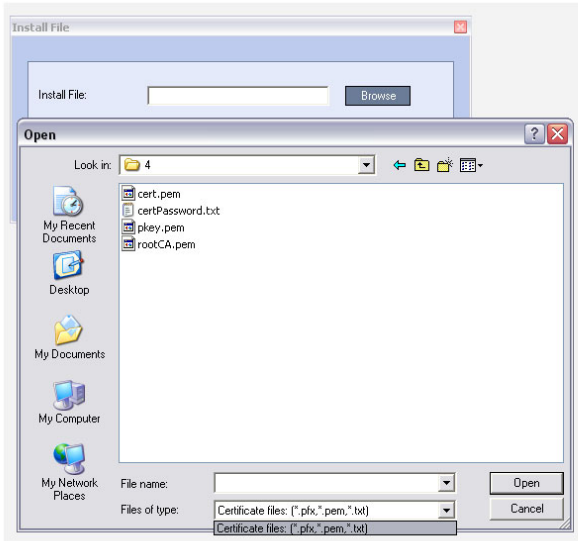
The PFX certificate request is created in the Microsoft Office Communications Server or Lync server. This certificate is received from the Certificate Authority it can be sent to the MCU, as described in the following procedure:

27 Click the **Send Certificate** button.



The *Install File* dialog box opens.

28 Click the **Browse** button.
The *Open* dialog box appears, letting you select the certificate file(s) to send to the MCU.



Depending on the method used when the certificate file(s) were created, send the certificate file(s) to the MCU according to the contents of the file set that was created:

— The certificate files *pkey.pem*, *cert.pem* and a *certPassword.txt*. The files were created by a Certificate Authority and are sent as is to the MCU together with the required password contained in the *certPassword.txt* file.
This is the recommended method.

— The files *pkey.pem* and *cert.pem*. The certificate files were created by a Certificate Authority and are sent as is to the MCU.

— A **.pfx* file and a *certPassword.txt* file. The file c*ertPassword.txt* is manually created if the **.pfx* file was created by the OCS using a password. The **.pfx* file will be converted internally by the MCU using the password included in the certPassword.txt into three certificate files named *pkey.pem* and *cert.pem*.

— A **.pfx* file if the certificate file was created in the OCS without using a password. The **.pfx* file will be converted internally by the MCU into three certificate files named *pkey.pem* and *cert.pem*.

29 In the file browser, select all files to be sent in one operation according to the contents of the set:

— One ***.pfx** file, or

— Two files: one ***.pfx** file and **certPassword.txt**, or

— Three files:**pkey.pem, cert.pem** and **certPassword.txt**

30 Click **Open**.
The selected file(s) appear in the *Install Files* path.

31 Click **Install**.
The files are sent to the MCU and the *Install File* dialog box closes.

32 In the *Default IP Service - Networking IP* dialog box, click **OK**.

33 In the *Reset Confirmation* dialog box, click **No** to modify the required system flags before resetting the MCU, or click **Yes** if the flag was already set**.**

> Reset can be performed after setting the system flags (for example, setting the MS_ENVIRONMENT flag). After system reset the MCU can register to the OCS server and make SIP calls.
> Sometimes the system fails to read the *.pfx file and the conversion process fails, which is indicated by the active alarm "SIP TLS: Registration server not responding" and/or "SIP TLS: Registration handshake failure". Sending *.pfx file again, as described in this procedure and then resetting the system may resolve the problem.

Polycom MCU System Flag Configuration

Enabling the Microsoft Environment

The MCU can be installed in Microsoft R2 environments. To adjust the MCU behavior to the Microsoft environment in each release, system flags must be set.

To configure the system flags on the Polycom MCU system:

1 On the *MCU* menu, click **Setup > System Configuration**.

The *System Flags - MCMS_PARAMETERS_USER* dialog box opens.

2 Scroll to the flag **MS_ENVIRONMENT** and click it.
The *Edit Flag* dialog box is displayed.

3 In the *Value* field, enter **YES** to set the MCU SIP environment to Microsoft solution.

> MCU set to MS_ENVIRONMENT=YES supports SIP over TLS only and not over TCP.

4 Click **OK** to complete the flag definition.

5 When prompted, click **Yes** to reset the MCU and implement the changes to the system configuration. After system reset the MCU can register to the OCS server and make SIP calls.

> Sometimes the system fails to read the *.pfx file and the conversion process fails, which is indicated by the active alarm "SIP TLS: Registration server not responding" and/or "SIP TLS: Registration handshake failure". Sending *.pfx file again, as described in this procedure and then resetting the system may resolve the problem.

In some configurations, the following flags may require modifications when **MS_ENVIRONMENT** flag is set to YES:

Table H-2 *Additional Microsoft Environment Flags in the MCU MCMS_PARAMETERS_USER Tab*

Flag Name	Value and Description
SIP_FREE_VIDEO_RESOURCES	Default value in Microsoft environment: **NO.** When set to NO, video resources that were allocated to participants remain allocated to the participants as long as they are connected to the conference even if the call was changed to audio only. The system does not allocate the resources to other participants ensuring that the participants have the appropriate resources in case they want to return to the video call. The system allocates the resources according to the participant's endpoint capabilities, with a minimum of one CIF video resource. When this flag is set to YES, video ports are dynamically allocated or released according to the in the endpoint capabilities. For example, when an audio Only call is escalated to Video and vice versa or when the resolution is changed.
SIP_FAST_UPDATE_INTERVAL_ ENV	Default setting is **0** to prevent the MCU from automatically sending an Intra request to all SIP endpoints. Enter **n** (where n is any number of seconds other than 0) to let the MCU automatically send an Intra request to all SIP endpoints every n seconds. It is recommended to set the flag to 0 and modify the frequency in which the request is sent at the endpoint level (as defined in the next flag).
SIP_FAST_UPDATE_INTERVAL_ EP	Default setting is **0** to prevent the MCU from automatically sending an Intra request to Microsoft OC endpoints only, every 6 seconds. Enter the number of seconds in which the MCU automatically sends Intra requests to Microsoft OC endpoints only.

Setting the audio protocol for the Microsoft Client running on a single core PC

By default, Microsoft Office Communicator R2 or Lync Clients are connected to conferences using the G.722.1 audio algorithm. However, when these clients are hosted on single processor workstations, they may experience audio quality problems when this algorithm is used.

The *System Flag* **FORCE_AUDIO_CODEC_FOR_MS_SINGLE_CORE** is used to force the use of a specific Audio algorithm such as G.711 when a *Microsoft Office Communicator R2* or *Lync Client* is detected as being hosted on a single core processor.

This flag can be set to:

- **AUTO** – No forcing occurs and the MCU negotiates a full set of Audio algorithm during capabilities exchange.

- **G711A/U** or **G722** – Set this flag value according to the hosting workstation capabilities. If the MCU detects single core host during capabilities exchange it will assign a *G.711* or *G.722* Audio algorithm according to the flag value.

Possible values: **AUTO, G711A, G711U, G722**

Default: **G711A**

Controlling Resource Allocations for Lync Clients Using the RTV Video Protocol

The number of resources used by the system to connect a Lync client with RTV is determined according to the conference line rate and the Maximum video resolution set in the *Conference Profile*.

In versions 7.6 and earlier, when conferences are set to line rates above 600 kbps, the MCU could allocate up to three video resources to Lync clients connecting using the RTV video protocol.

From version 7.6.1, the system flag **MAX_RTV_RESOLUTION** enables you to override the MCU resolution selection and limit it to a lower resolution. Resource usage can then be minimized the 1 or 1.5 video resources per call instead of 3 resources, depending on the selected resolution.
Possible flag values are: **AUTO** (default), **QCIF**, **CIF**, **VGA** or **HD720**.

For example, if the flag is set to VGA, conference line rate is 1024Kbps, and the Profile Maximum Resolution is set to Auto, the system will limit the Lync RTV client to a resolution of VGA instead of HD720p and will consume only 1.5 video resources instead of 3 resources.

When set to **AUTO** (default), the system uses the default resolution matrix based on the conference line rate.

To change the default flag setting, add the MAX_RTV_RESOLUTION flag to the *System Configuration* flags and set its value. For information, see .

The following table summarizes the MCU resources allocated to a Lync Client based on the MAX_RTV_RESOLUTION flag setting, the connection line rate and the video resolution.

Table H-3 *Selected video resolution based on flag setting and conference line rate and core processor*

Maximum Resolution Value	Line Rate	Selected Video Resolution Per Core Processor		
		Quad	Dual	Single
AUTO	> 600 kbps	HD720p 30fps	VGA 30fps	VGA 15fps
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
HD720p	> 600 kbps	HD720p 30fps	HD720p 13fps	VGA 15fps
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF

Table H-3 Selected video resolution based on flag setting and conference line rate and core processor (Continued)

Maximum Resolution Value	Line Rate	Selected Video Resolution Per Core Processor		
		Quad	Dual	Single
VGA	> 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
CIF	> 600 kbps	CIF	CIF	CIF
	250 kbps - 600 kbps	CIF	CIF	CIF
	180 kbps - 249 kbps	CIF	CIF	CIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF
QCIF	> 600 kbps	QCIF	QCIF	QCIF
	250 kbps - 600 kbps	QCIF	QCIF	QCIF
	180 kbps - 249 kbps	QCIF	QCIF	QCIF
	64 kbps - 179 kbps	QCIF	QCIF	QCIF

When the MAX_ALLOWED_RTV_HD_FRAME_RATE flag equals 0 (default value), Table 1-1 for the MAX_RTV_RESOLUTION flag applies. When the MAX_ALLOWED_RTV_HD_FRAME_RATE flag does not equal 0, see "*Threshold HD Flag Settings using the RTV Video Protocol"* on page **3-30** for more information.

The following table describes the number of allocated video resources for each video resolution when using the RTV protocol.

Table H-4 Allocated video resolutions per video resolution

Selected Video Resolution	Number of Allocated Video Resources
HD720p	3
VGA	1.5
CIF	1
QCIF	1

HD Frame Rate Flag Settings using the RTV Video Protocol

The system flag **MAX_ALLOWED_RTV_HD_FRAME_RATE** defines the threshold Frame Rate (fps) in which RTV Video Protocol initiates HD resolutions.

Flag values are as follows:

- Default: **0** (fps) - Implements any Frame Rate based on Lync RTV Client capabilities

> If the MAX_RTV_RESOLUTION flag is set to AUTO dual core systems always view VGA. For more information on Lync RTV Client capabilities, see , *"Controlling Resource Allocations for Lync Clients Using RTV Video Protocol"* on page **3-27** for more information.

- Range: **0-30** (fps)

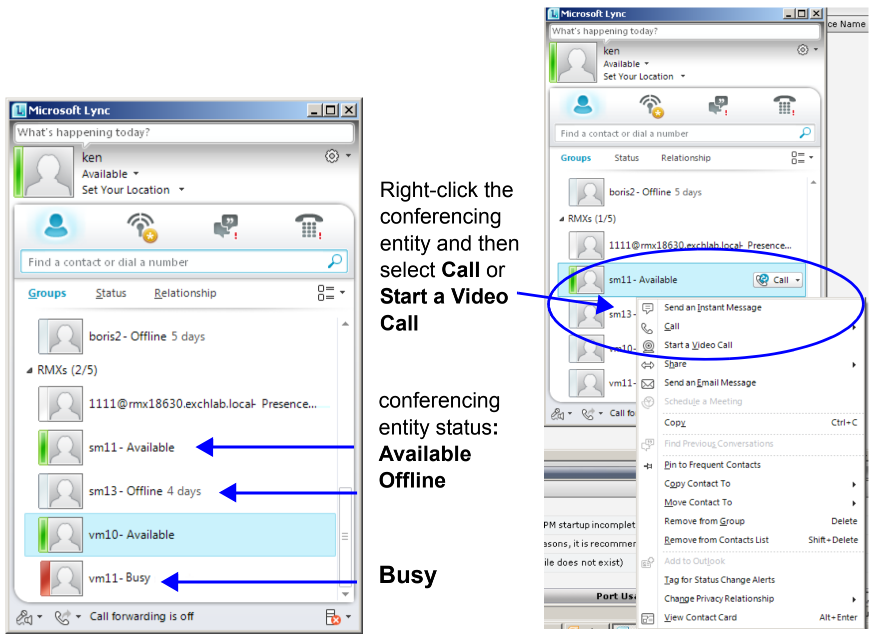
For example, when the flag is set to 15 and the Lync RTV Client declares HD 720P at 10fps, because the endpoint's frame rate (fps) of 10 is less than flag setting of 15, then the endpoint's video will open VGA and not HD.

In another example, when the flag is set to a frame rate of 10 and the Lync RTV Client declares HD 720P at 13fps, because the endpoint's frame rate (fps) of 13 is greater than flag setting of 10, then the endpoint's video will open HD and not VGA.

> - Single core PC's cannot view HD and always connect in VGA.
> - Dual Core Processor - The threshold for flag settings on Dual Core systems is 13 (fps) and less for viewing HD. When system flag is set to 14 (fps) or higher, the RTV Video Protocol shall connect in VGA.
> - Quad Core PC systems always view HD, even when flag settings are set anywhere from to 0-30.
> - The number of resources used by the system to connect a Lync client with RTV is determined according to the conference line rate and the maximum video resolution set in the Conference Profile. For more information, see *"Microsoft RTV Video Protocol Support in CP Conferences"* on page **3-24**.

Adding Presence to Conferencing Entities in the Buddy List

Registration of conferencing entities (Meeting Rooms, Entry Queues and SIP Factories) with the SIP server adds these conferencing entities to the buddy list with their presence. It enables the Office Communication Server client or LYNC Server client users to see the availability status (Available, Offline, or Busy) of these conferencing entities and connect to them directly from the buddy list.



Guidelines

- Registration with Presence of up to 100 conferencing entities to a single SIP Server is supported. When this number is exceeded, the additional conferencing entity may appear to be successfully registered but the presence status will be shown as 'Offline' in Lync for any entities beyond the limit.
- Lync endpoints cannot connect to conferencing entities that their presence is “offline”.
- The Conferencing Entity (Meeting Room or Entry Queue or SIP Factory) has to be added to the Active Directory as a User.

  Make sure that a unique name is assigned to the conferencing entity and it is not already used for another user account in the Active Directory.
- The conferencing entity name must not include any upper case letters.
- When the MCU system is shutting down while a Meeting Room is still active, as indicated by its presence, the status remains active for 10 minutes during which Lync endpoints cannot connect to the Meeting Room. After 10 minutes, the Meeting Room Status changes to “offline”.
- From Version 7.1, registration of the conferencing entity is defined in the Conference Profile (and not in the IP Network Service), enabling you to choose the conferencing entity to register.

- In *Multiple Networks* configuration, an IP Network Service that is enabled for registration in a Conference Profile cannot be deleted.
- Upgrading from previous versions to version 7.1 and later requires manual update of the registration in the Conference Profiles that are assigned to the conferencing entities.

Enabling the Registration of the Conferencing Entities

The creation of the various conferencing entities is described in the following chapters:

- "*Meeting Rooms*" on page **6-1**
- "*Entry Queues, Ad Hoc Conferences and SIP Factories*" on page **7-1**

Registration with presence of conferencing entities with the SIP Server is enabled by performing the following processes:

- Creating an Active Directory Account for the Conferencing Entity.
- Enabling the Conferencing Entity User Account for Office Communication Server or Lync Server
- Defining the Microsoft SIP Server in the IP Network Service
- Enabling Registration in the Conference Profile

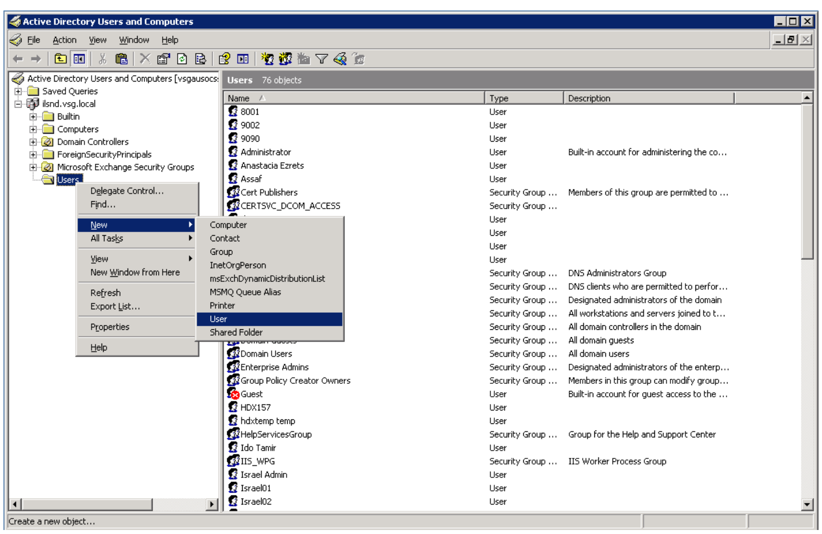
Creating an Active Directory Account for the Conferencing Entity

The User account created for the Conferencing entity is used for registration with the Office Communication Server or Lync server and to automatically synchronize with the STUN and relay (Edge) servers.

To add the conferencing entity user to the Active Directory:

1 Go to **Start > Run** and enter **dsa.msc** to open the *Active Directory Users and Computers* console.

2 In the console tree, select **Users > New > User**.



3 In the *New User* wizard, define the following parameters:

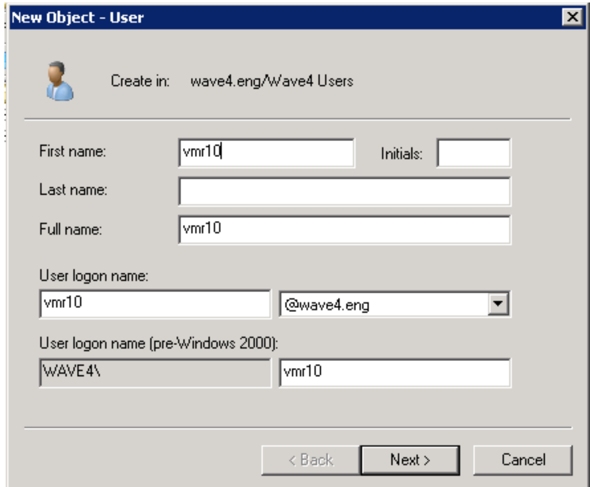


Table H-5 Active Directory - New User Parameters for the MCU

Field	Description
First Name	Enter the name of the conferencing entity user. This name will appear in the buddy list of the Office Communication Server or Lync server. For example, vmr10. **Notes:** • This name must be the identical to the **Routing Name** assigned to the conferencing entity in the MCU system. It must also be the *User Login Name* in the Active Directory. • The name can include only lower case characters and/or numbers.
Full Name	Enter the same name as entered in the *First Name* field.
User Login Name	Enter the same name as entered in the *First Name* field and select from the drop down list the domain name for this user. It is the domain name defined for the Office Communication Server or Lync server.

4 Click **Next**.

5 Enter the password that complies with the Active Directory conventions and confirm the password.

6 Select the options: **User cannot change password** and **Password never expires**. Clear the other options.

7 Click **Next**.
The system displays summary information.

8 Click **Finish**.

The new User is added to the Active Directory *Users* list.

9 Repeat for each MCU conferencing entity.

Enabling the Conferencing Entity User Account for Office Communication Server or Lync Server

The new Conferencing Entity user must be enabled for registration with the Office Communications Server or Lync Server.

To enable the Conferencing Entity User Account for Office Communication Server:

1 In the *Active Directory Users and Computers* window, right-click the conferencing entity user and then click **Properties**.

2 In the *Properties* dialog box, click the **Communications** tab.

3 In the *Sign in name* field, enter the conferencing entity user name in the format **SIP:conferencing entity user name** (for example sip:vm10) and select the domain name (for example, lab.vsg.local) as entered in the *New User* dialog box.

4 Select the *Server or Pool* from the list.

5 Click **Apply** and then **OK**.

To enable the Conferencing Entity User Account for Lync Server:

1 On the computer running the Lync Server 2010, go to **Start->All Programs->Microsoft Lync Server 2010>Lync Server Control Panel**.

   Windows Security window opens.

2 Enter your User name and Password as configured in the Lync Server and click OK. The *Microsoft Lync Server 2010 Control Panel* window opens.

3 Click the **Users** tab.

4 In the *User Search* pane, click the **Enable Users** heading.

   The *New Lync Server User* pane opens.

5 Click the **Add** button.

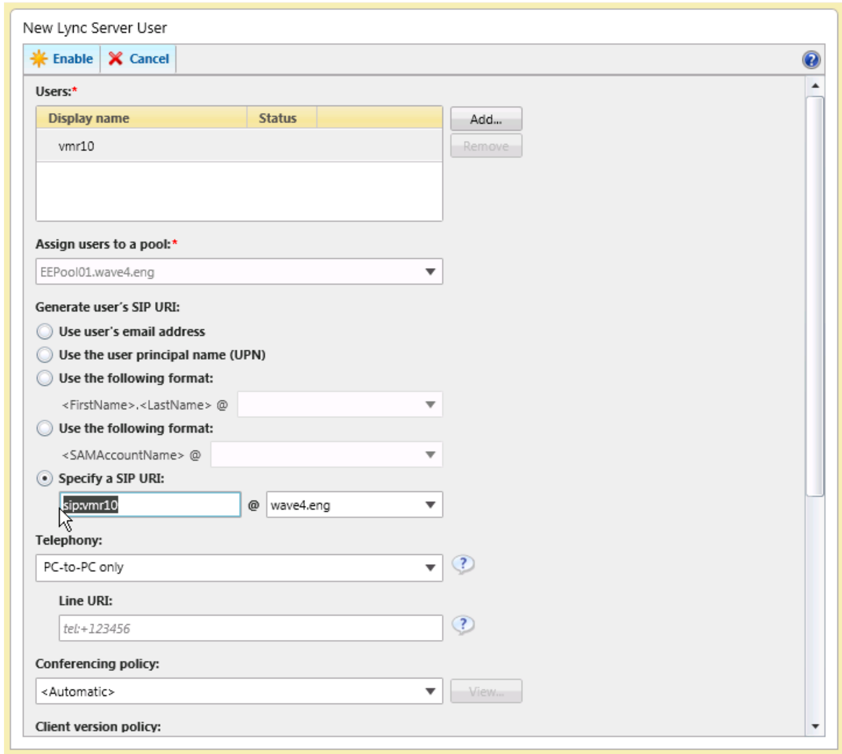
   The *Select from Active Directory* dialog box opens.

6 Enter the conferencing entity user name as defined in the Active Directory, and then click the **Find** button.

   The requested user is listed in the *Select From Active Directory* dialog box.

7 Select the listed user (conferencing entity user) and click **OK**. The selected user appears in the *New Lync Server User* pane.

8 Select the following parameters:



— In *Assign users to a pool* field, select the required pool.

— In the *Generate user SIP URI*, define the SIP URI of the conferencing entity using one of the following methods:

- Select the **Specify a SIP URI** option and enter the conferencing entity user portion of SIP URI defined in the active directory. This SIP URI must match the conferencing entity Routing Name configured in MCU. For example, for the meeting room account **sip:vmr10@wave4.eng**, use only the **vmr10** portion of the address.

or

- Select the **Use the user principal name (UPN)** option.

9 Click the **Enable** button.
The selected user appears as enabled in the *User Search* pane.

Defining the Microsoft SIP Server in the IP Network Service

To enable the registration of the conferencing entities the *SIP Server Type* must be set to **Microsoft** and the Office Communication Server or Lync Server properties in the *IP Network Service - SIP Servers* dialog box.

For more details, see "*Configuring the MCU IP Network Service"* on page **H-38**.

Enabling Registration in the Conference Profile

Registration of conferencing entities such as ongoing conferences, *Meeting Rooms, Entry Queues, SIP Factories* and *Gateway Sessions* with *SIP* servers is done per conferencing entity. This allows better control on the number of entities that register with each *SIP* server.

Selective registration is enabled by assigning a conference Profile in which registration is enabled to the conferencing entities that require registration. Assigning a conference Profile in which registration is disabled (registration check box is cleared) to conferencing entities will prevent them from registering. By default, Registration is disabled in the Conference Profile, and must be enabled in Profiles assigned to conferencing entities that require registration.

Registration can be enabled in the *New Profile - Network Services* dialog box:

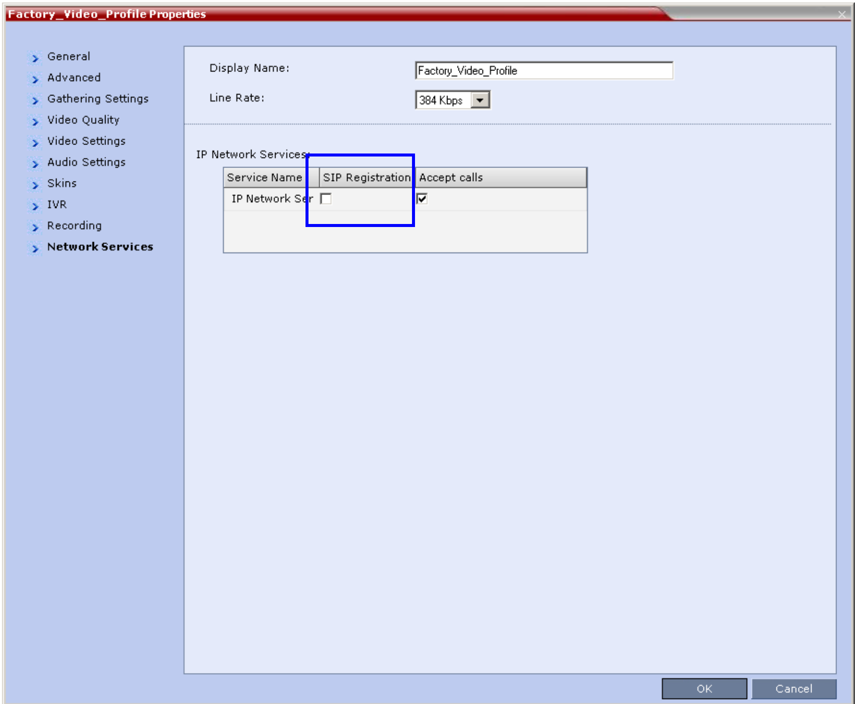


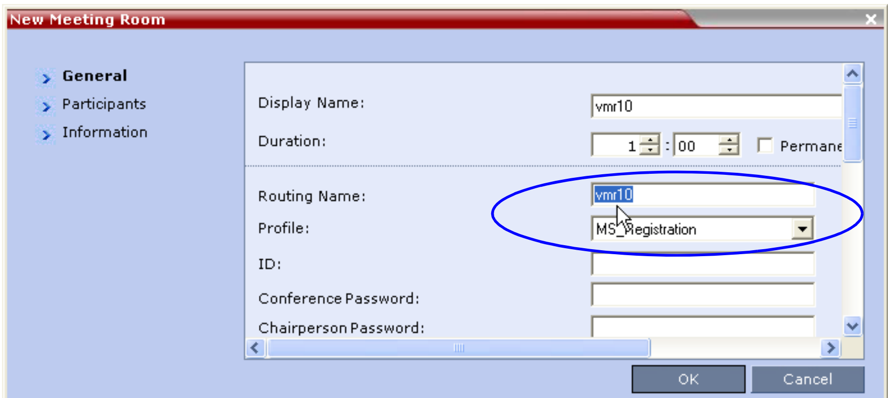
Table H-6 *Profile Properties - Network Services*

Parameter	Description
IP Network Services:	
Service Name	This column lists all the defined *Network Services,* one or several depending on the system configuration (single Network or Multiple Networks).
SIP Registration	To register the conferencing entity to which this profile is assigned, with the SIP Server defined for that *Network Service*, click the *SIP Registration* check box of that *Network Service*.
Accept Calls	To prevent dial in participants from connecting to a conferencing entity when connecting via a certain *Network Service*, clear the *Accept Calls* check box of that *Network Service*.

Verifying the MCU Conferencing Entity Routing Name and Profile

MCU conferencing entity can be dialed directly from the buddy list of the Office Communications client or the Lync client if its routing name matches the user name of Active Directory account you created and Registration is enabled in the Conference Profile assigned to it.

- To ensure that the MCU meeting room or conferencing entity is properly configured for registration the following parameters must be defined:
  - The user name on the conferencing entity in Active Directory account must be identical to its **Routing Name** on the MCU.
    For example, if the SIP URI in the Active Directory is **`sip:vmr10@wave4.eng`**, it must be defined as **`vmr10`** in the *Routing Name* field of that MCU conferencing entity.



  - In the *Profile* field, make sure that a conference Profile that has been enabled for SIP registration is selected.

Monitoring the Registration Status of a Conferencing Entity in the RealPresence Collaboration Server (RMX) Web Client or RMX Manager Application

The Status of the SIP registration can be viewed in the appropriate conferencing Entity list or when displaying its properties.

Conferencing Entity List

The list of conferencing entity includes an additional column - *SIP Registration,* which indicates the status of its registration with the SIP server. The following statuses are displayed:

- **Not configured** - Registration with the SIP Server was not enabled in the Conference Profile assigned to this conferencing Entity. In Multiple Networks configuration, If one service is not configured while others are configured and registered, the status reflects the registration with the configured Network Services. The registration status with each SIP Server can be viewed in the *Properties - Network Services* dialog box of each conferencing entity.

  When SIP registration is not enabled in the conference profile, the MCU's registering to SIP Servers will each register with an URL derived from its own signaling address. This unique URL replaces the non-unique URL, dummy_tester, used in previous versions.
- **Failed** - Registration with the SIP Server failed.
  This may be due to incorrect definition of the SIP server in the IP Network Service, or

the SIP server may be down, or any other reason the affects the connection between the MCU or the SIP Server to the network.

- **Registered** - the conferencing entity is registered with the SIP Server.
- **Partially Registered** - This status is available only in Multiple Networks configuration, when the conferencing entity failed to register to all the required Network Services (if more than one Network Service was selected for Registration). The registration status with each SIP Server can be viewed in the *Properties - Network Services* dialog box of each conferencing entity.

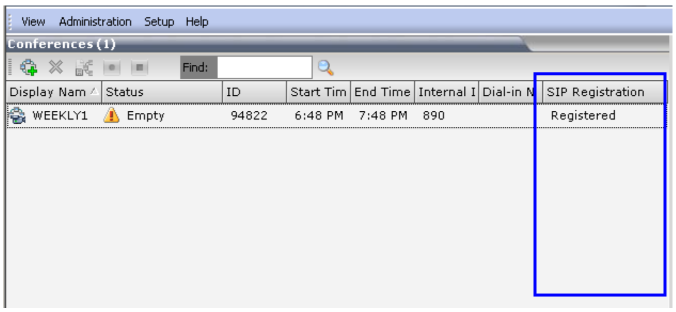


Figure H-3 Ongoing Conferences list - SIP Registration

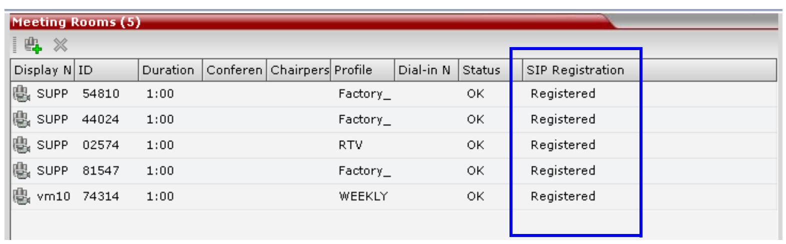


Figure H-4 Meeting Rooms list - SIP Registration

Figure H-5 Entry Queues list - SIP Registration

Figure H-6 SIP Factories list - SIP Registration

Conferencing Entity Properties

Registration status is reflected in the *Properties - Network Services* dialog box:

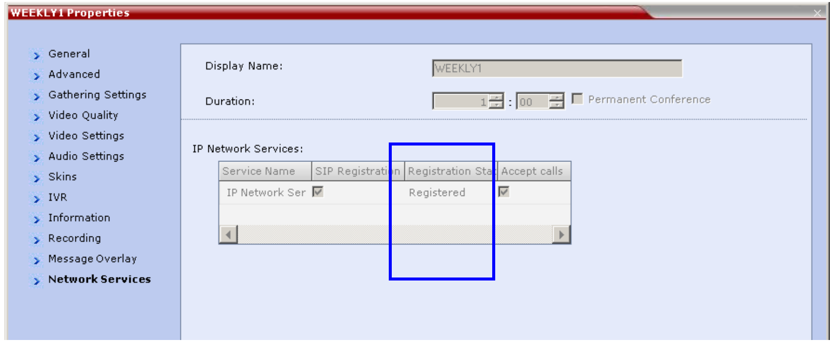


Figure H-7 *Ongoing conference Properties - Network Services - SIP Registration*

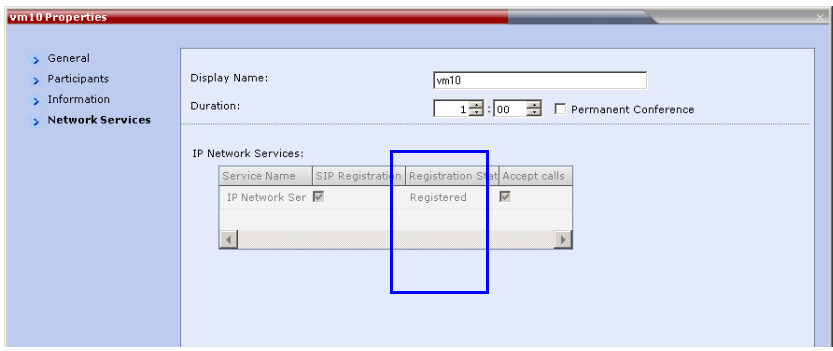


Figure H-8 *Meeting Room Properties - Network Services - SIP Registration*

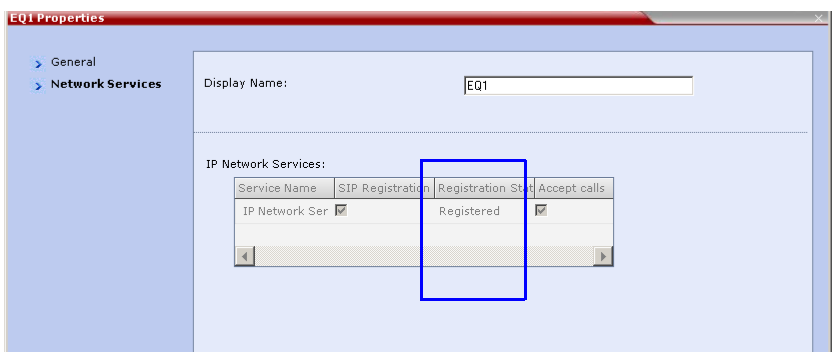


Figure H-9 *Entry Queue Properties - Network Services - SIP Registration*

MCU Configuration for CAC Implementation

Enabling CAC Implementation

CAC is enabled by manually adding the flags to the system Configuration and setting their values as follows:

- To enable the Call Admission Control implementation in the MCU:
  — **CAC_ENABLE=YES**
- In addition, to ensure that endpoints such as HDX remain connected to the conference for its duration when the RMX is configured with FQDN address and the Lync server is working with load balancing and holds more than one address, the following two flags must be manually added and set to:
  — **MS_KEEP_ALIVE_ENABLE = YES**
  Note: Since the keep alive is only required when the Lync server is working with load balancing and holds more than one address, the default value is NO.
  — **SIP_TCP_PORT_ADDR_STRATEGY = 1** (default setting)
- When Call Admission Control is enabled in the local network, by default the local the ICE channel is closed after applying CAC bandwidth management.
  To change and preserve the ICE channel open throughout the call:
  — **PRESERVE_ICE_CHANNEL_IN_CASE_OF_LOCAL_MODE=YES**.

Conferencing Behavior

Continuous Presence Conferences

In Continuous Presence conference, Lync clients connect with any allocated bandwidth.

Video Switching Conferences

In Video Switching conferences, Lync clients must connect with the same line rate as the conference, otherwise they will be connected as Secondary (Audio Only) participants.

Mitigation of the line rate requirement can be effected by modifying the system flag: **VSW_RATE_TOLERANCE_PERECENT**.

This system flag determines the line rate tolerance.
Possible values are: **0 - 75**.

Setting this flag to **0** (0% - default) determines no line rate tolerance and the participant must connect at the conference line rate.

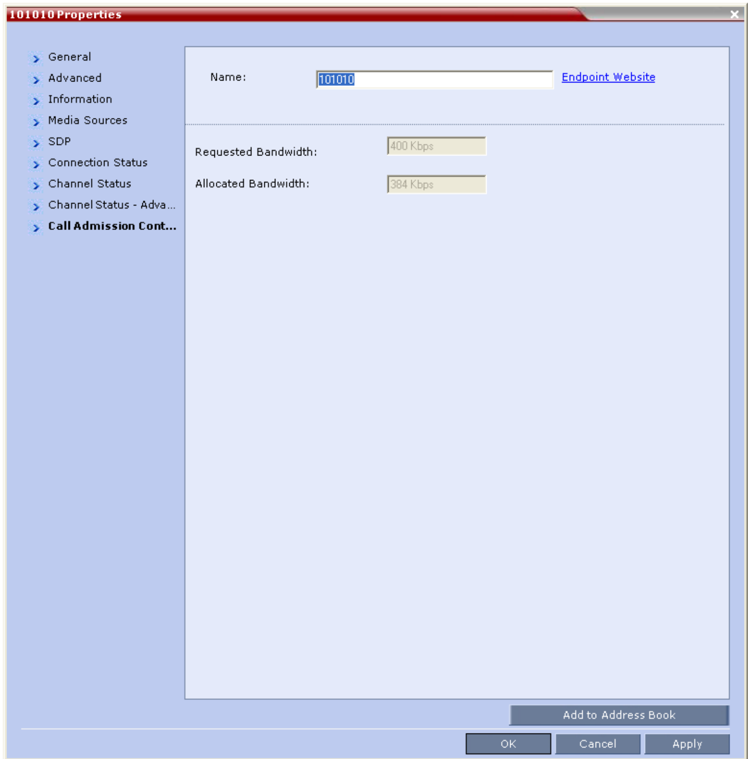
Setting this flag to a value between 1 and 75 determines the percentage of bandwidth that can be deducted from the required bandwidth to allow participants to connect to the conference.
For example, if you enter 20 (for 20%) as the flag value, the participant will be able to connect to the conference if the allocated line rate is up to 20% lower than the conference line rate (or between 80% to 100% of the required bandwidth). If the conference line rate is 1024Kbps, participant with a line rate between 819Kbps and 1024Kbps will be able to connect to the conference.

When a tolerance is set, the Highest Common mechanism is enabled for the conference line rate. When a participant with a lower line rate connects to the conference, the line rate of all other connected participants is reduced accordingly and when that participant disconnects from the conference, the line rate of the remaining participants is increased to the highest possible rate common to all connected participants.

For example, if a participant with a line rate of 900Kbps connects to the conference to which all other participants are connected at a line rate of 1024kbps, the line rate of all participants will decrease to 900Kbps. When this participant disconnects, the line rate of the remaining participants will increase to 1024Kbps.

Monitoring Participant Connections

Activation of the Call Admission Control for a call can be viewed in the *Participant Properties - Call Admission Control* dialog box.



This information applies only to dial-in participants.
The following information is available:

Table H-7 *Participant Properties - Call Admission Control Parameters*

Field	Description
Requested Bandwidth	Indicates the bandwidth requested by the Lync client (usually the line rate set for the conference). NA - indicates that *Call Admission Control is disabled.*
Allocated Bandwidth	The actual bandwidth allocated by the Lync Policy Server. NA - indicates that *Call Admission Control is disabled.*

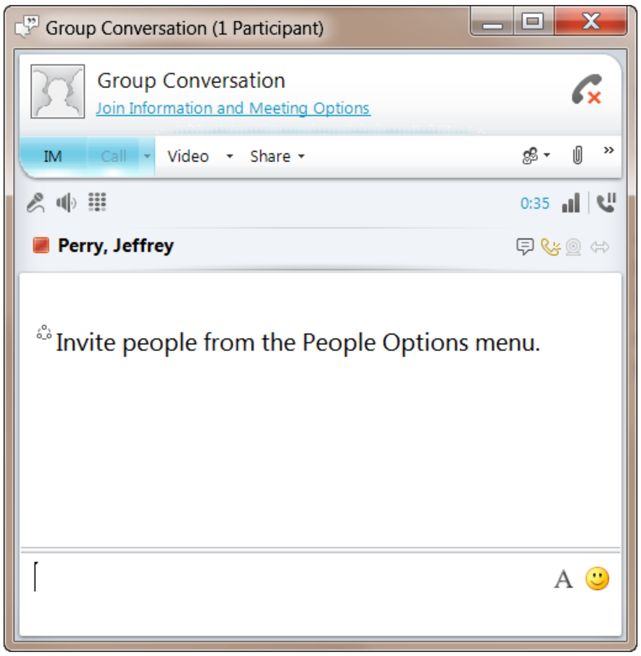
Connecting an MCU Meeting Room to a Microsoft AV-MCU Conference

Microsoft Lync users can connect an MCU Meeting Room to a conference running on the Microsoft A/V MCU. This allows MCU Lync users to connect with a conference in progress on the A/V MCU and be an active participant in the conference. The connection to the A/V MCU is the same configuration as a cascading conference between multiple MCU MCUs.

To connect to an A/V MCU conference:

1 From the Menu bar, click **Meet Now** to create an ad-hoc conference.

The Group Conversation dialog box is displayed.



2 From the Contacts List on Lync, drag a Virtual Meeting Room (VMR) into the Group Conversation list.

After the Virtual Meeting Room is connected on Lync, an invitation is sent from the A/V MCU to the MCU using the Centralized Conference Control Protocol (CCCP). The MCU responds and triggers a standard SIP invite sent from the A/V MCU to the MCU.

Multiple participants can now connect to both the MCU Meeting Room and the A/V MCU, and participate in a cascaded conference.

When a conference begins with Audio Only, a Lync user cannot add video to the conference after the VMR is connected to the conference. The conference will remain as Audio Only.

Configuring the MCU for Federated (ICE) Dialing

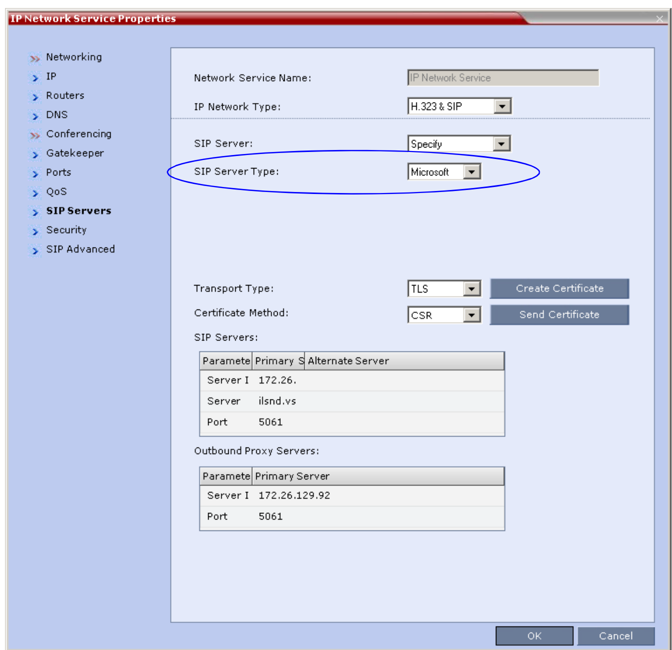
The MCU *Default IP Network Service* must be configured to work with the Office Communication Server/Lync Server as the SIP Server and the MCU user defined in the Active Directory must also be defined in the MCU ICE environment parameters to enable remote dialing in a federated (ICE) environment, .

> The procedure described here assumes that the MCU is configured to work in Microsoft environment as described in "*Configuring the RMX 1500/2000/4000 for Microsoft Integration"* on page **H-36**.

To configure the MCU for ICE Dialing:

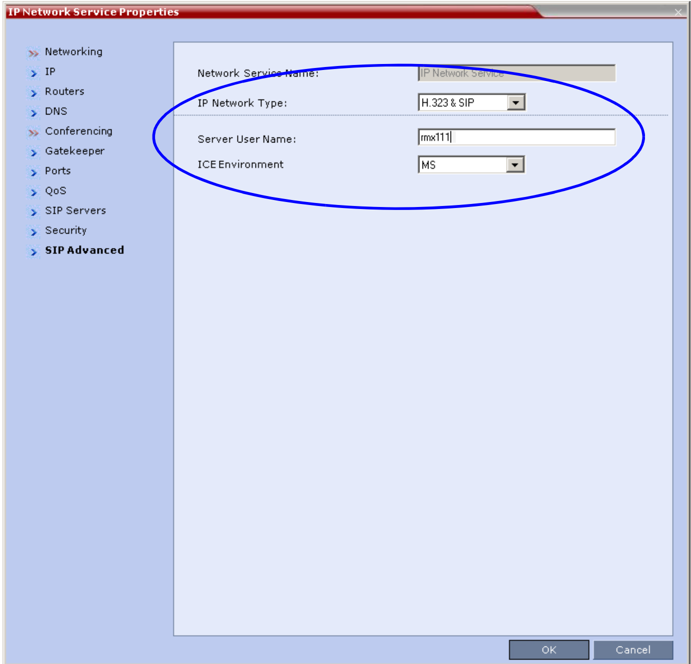
1. In the RealPresence Collaboration Server Web browser, in the *RMX Management* pane, expand the **Rarely Used** list and click **IP Network Services** ( ).
2. In the *IP Network Services* pane, double-click the **Default IP Service** (, , or) entry.

   The *Default IP Service - Networking IP* dialog box opens.
3. Click the **SIP Servers** tab.



4. Make sure that the *SIP Server* is set to **Specify.**
5. Make sure that the *SIP Server Type* is set to **Microsoft**.
6. Make sure that the IP address of the Office Communications Server 2007 or Lync Server 2010 is specified and the *Server Domain Name* is the same as defined in the OCS/Lync Server and in the *Management Network* for the DNS.

7 Click the **SIP Advanced** tab.



8 In the *ICE Environment* field, select **MS** (for Microsoft ICE implementation) to enable the ICE integration.
This field is disabled if the MCU is running in *MPM Card Configuration Mode*.

9 In the *Server User Name* field, enter the MCU User name as defined in the Active Directory. For example, enter **rmx111**.
This field is disabled if the *ICE Environment* field is set to **None**.

10 **Optional** if the **Fixed Ports** options was selected previously.
Click the **Ports** tab to modify the number of UDP Ports allocated to the calls to accommodate the number of ports required for ICE dialing.

11 In the *UDP Port Range*, modify the number of UDP ports by enter the first and last port numbers in the range. When ICE environment is enabled, the number of ports defined in the range should be **2024**.

12 Click **OK**.
The MCU will register with the OCS/Lync Server enabling automatic retrieval of the STUN server and Relay server parameters for ICE dialing.

These parameters can be viewed in the *Signaling Monitor - ICE Servers* dialog box.

Monitoring the Connection to the STUN and Relay Servers in the ICE Environment

1 In the MCU Web browser, in the *MCU Management* pane, click **Signaling Monitor**.

2 In the *Signaling Monitor* pane, click the **IP Network Service** entry.

3 Click the **ICE Servers** tab.

The system lists the ICE servers to which it is connected and the status of the connection of each of the MCU media cards (status 1, status 2, etc) to ICE servers. (One status is displayed for RealPresence Collaboration Server (RMX) 1500, two statuses are displayed for RealPresence Collaboration Server (RMX) 2000 and four statuses are displayed for RealPresence Collaboration Server (RMX) 4000).

It addition, the system indicates the status of the firewall detection in the MCU.

Monitoring the Participant Connection in ICE Environment

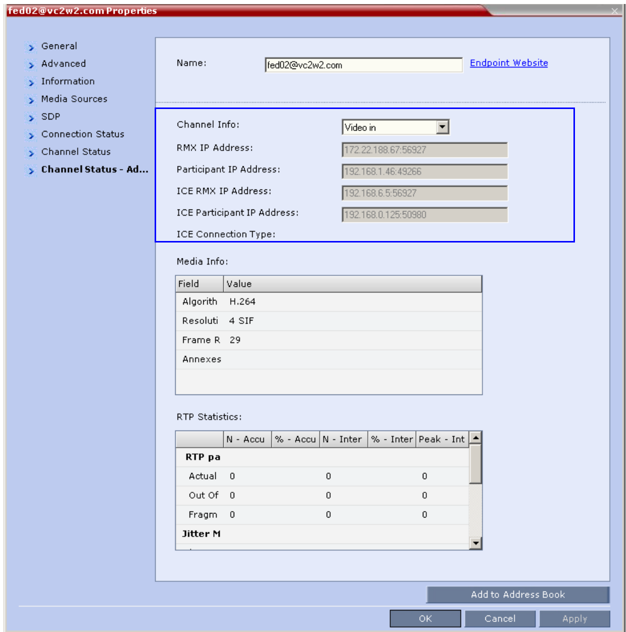
For each participant in the conference running in ICE environment, you can view the local and the external IP addresses and the type of connection between the MCU and the participant (remote).

The ICE information is displayed only for the media channels and not the signaling channel.

To view the channel properties of the participant:

1 In the participants pane, double-click the participant entry or right-click the participant entry and then click **Properties**.

2 Click the **Channel Status - Advanced** tab.



The following connection information is displayed:

***Table H-8** Participant Properties - ICE Connection Parameters*

Field	Description
MCU IP Address	The local IP address and port (in the format IP address:Port) of the MCU.
Participant IP Address	The local IP address and port (in the format IP address:Port) of the endpoint.
ICE MCU IP Address	The IP address and the Port number of the MCU used to pass through the media. This information changes according to the *ICE connection type:* • When *ICE connection type* is **local**, it is identical to the IP address:Port displayed in the *MCU IP Address.* • When *ICE connection type* is **relay**, the system displays the IP address and port number of the relay server used to pass the media from the MCU to the participant. • When *ICE connection type* is **firewall**, the system displays the public IP address and port of the MCU as seen outside the private network.

Table H-8 Participant Properties - ICE Connection Parameters (Continued)

Field	Description
ICE Participant IP Address	The IP address and the Port number of the endpoint used to pass through the media. This information changes according to the *ICE connection type:* • When *ICE connection type* is **local**, it is identical to the IP address:Port displayed in the *Participant IP Address.* • When *ICE connection type* is **relay**, the system displays the IP address and port number of the relay server used to pass the media from the participant to the MCU. • When *ICE connection type* is **firewall**, the system displays the public IP address and port of the endpoint as seen outside the private network.
ICE Connection Type	Indicates the type of connection between the MCU and the participant in the ICE environment: • **Local** (or Host) - The endpoint (Remote) is on the same network as the MCU and the media connection is direct, using local addresses. • **Relay** - Media between the MCU and the participant passes through a media relay server. • **Firewall** - Media connection between the MCU and the participant is done using their external IP addresses (the IP addresses as seen outside of the local network).

For detailed description of ICE Active alarms, see "*ICE Active Alarms"* on page **H-69**.

Active Alarms and Troubleshooting

Active Alarms

The following active alarms may be displayed in the MCU *System Alerts* pane when the MCU is configured for integration in the OCS environment:

Table H-9 New Active Alarms

Alarm Code	Alarm Description
SIP TLS: Failed to load or verify certificate files	This alarm indicates that the certificate files required for SIP TLS could not be loaded to the MCU. Possible causes are: • Incorrect certificate file name. Only files with the following names can be loaded to the system: rootCA.pem, pkey.pem, cert.pem and certPassword.txt • Wrong certificate file type. Only files of the following types can be loaded to the system: rootCA.pem, pkey.pem and cert.pem and certPassword.txt • The contents of the certificate file does not match the system parameters

Table H-9 *New Active Alarms (Continued)*

Alarm Code	Alarm Description
SIP TLS: Registration transport error	This alarm indicates that the communication with the SIP server cannot be established. Possible causes are: • Incorrect IP address of the SIP server • The SIP server listening port is other than the one defined in the system • The OCS services are stopped **Note:** Sometimes this alarm may be activated without real cause. Resetting the MCU may clear the alarm.
SIP TLS: Registration handshake failure	This alarm indicates a mismatch between the security protocols of the OCS and the MCU, preventing the Registration of the MCU to the OCS.
SIP TLS: Registration server not responding	This alarm is displayed when the MCU does not receive a response from the OCS to the registration request in the expected time frame. Possible causes are: • The MCU FQDN name is not defined in the OCS pool, or is defined incorrectly. • The time frame for the expected response was too short and it will be updated with the next data refresh. The alarm may be cleared automatically the next time the data is refreshed. Alternatively, the OCS Pool Service can be stopped and restarted to refresh the data. • The MCU FQDN name is not defined in the DNS server. Ping the DNS using the MCU FQDN name to ensure that the MCU is correctly registered to the DNS.
SIP TLS: Certificate has expired	The current TLS certificate files have expired and must be replaced with new files.
SIP TLS: Certificate is about to expire	The current TLS certificate files will expire shortly and will have to be replaced to ensure the communication with the OCS.
SIP TLS: Certificate subject name is not valid or DNS failed to resolve this name	This alarm is displayed if the name of the MCU in the certificate file is different from the FQDN name defined in the OCS. **Note:** Occasionally this alarm may be activated without real cause. Resetting the MCU may clear the alarm.

ICE Active Alarms

When ICE environment is enabled in the MCU, failure to communicate with a required component triggers the display of an Active Alarm in the System Alerts pane.

The following table lists these active alarms:

Table 9 *ICE Environment - MCU Active Alarms*

Active Alarm	Phase	Alarm Displayed When	Troubleshooting
ICE failure: Failed to register with OCS. Check the MCU Server Name.	Registration	The MCU did not receive a confirmation response from the OCS to the Registration request.	• Check that the MCU Server Name in IP Network Service - SIP Advanced is identical to the User name defined for the MCU in the OCS Active Directory. • Make sure that the MCU user is defined in the OCS Active Directory.
ICE failure: Failed to subscribe with the OCS, therefore the A/V Edge Server URI was not received.	Subscribe	The MCU did not receive a confirmation response from the OCS to the Subscription request. The Subscription is required for obtaining the A/V Edge Server URI which is followed by the notify message containing the credentials).	
ICE failure: The Notify message containing the A/V Edge Server URI was not received	Notify	The Notify message containing the A/V Edge Server URI was not received by the MCU.	
ICE failure: Received Notification does not contain URI.	Notify	The notify message that was sent from the A/V Edge Server does not contain the A/V Edge server URI.	Verify the A/V Edge server is configured in the OCS.
ICE failure: No response from the A/V Edge Server to the MCU Service Request	Service	The MCU did not receive a confirmation response from the A/V Edge Server to the Service request.	
ICE failure: Received Service message does not contain the Credentials.	Service	The Service message response does not contain the Credentials.	

Table 9 ICE Environment - MCU Active Alarms

Active Alarm	Phase	Alarm Displayed When	Troubleshooting
ICE failure: A/V Edge server URI cannot be resolved	Service	The MCU failed to resolve The remote address of the Edge server URI.	
ICE failure: Service credential denied. A/V Edge server credentials rejected by the OCS.	Service	This alarm indicates that the OCS does not configure with the. Generated by the ICE stack.	

Troubleshooting

- At the end of the installation and configuration process, to test the solution and the integration with the OCS, create an ongoing conference with two participants, one dial-in and one dial-out and connect them to the conference.
- If the *active* Alarm *"SIP TLS: Registration server not responding"* is displayed, stop and restart the OCS Pool Service.
- If the communication between the OCS and the MCU cannot be established, one of the possible causes can be that the MCU FQDN name is defined differently in the DNS, OCS and MCU. The name must be defined identically in all three devices, and defined as type A in the DNS. The definition of the MCU FQDN name in the DNS can be tested by pinging it and receiving the MCU signaling IP from the DNS in return.
- The communication between the OCS and the MCU can be checked in the Logger files:
  — SIP 401/407 reject messages indicate that the MCU is not configured as Trusted in the OCS and must be configured accordingly.
  — SIP 404 reject indication indicates that the connection to the OCS was established successfully.

Known Issues

- Selecting **Pause my Video** in OC client causes the call to downgrade to audio only call if the call was not in Audio Only mode at all (the call was started as a video call).

  If the call is started as an audio only call and video is added to it, or if the call was started as video call and during the call it was changed to Audio Only and back to video, selecting *Pause my Video* will suspend it as required.
- Rarely, the OC client disconnects after 15 minutes. The OC client can be reconnected using the same dialing method in which they were previously connected (dial-in or dial-out).
- Rarely, all SIP endpoints disconnect at the same time. The SIP endpoint can be reconnected using the same dialing method in which they were previously connected (dial-in or dial-out).

Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners. These additional services will help customers successfully design, deploy, optimize and manage Polycom visual communications within their UC environments.

Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. For additional information and details please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Appendix I

Polycom Open Collaboration Network (POCN)

Working in the Open Collaboration Server and TIP protocol are supported in AVC Conferencing Mode only.

Collaboration With Cisco's Telepresence Interoperability Protocol (TIP)

TIP is a proprietary protocol created by *Cisco* for deployment in *Cisco TelePresence systems (CTS)*. Since *TIP* is not compatible with standard video communication systems, interoperability between *Cisco* and other vendors' telepresence systems was initially impossible.

Gateways were developed to provide interoperability but were subject to the inherent problems of additional latency (delay) in connections and low video quality resulting from the reformatting of video and audio content.

Polycom's solution is to allow the MCU to natively inter-operate with *Cisco TelePresence Systems*, ensuring optimum quality multi-screen, multipoint calls between:

- *Polycom Immersive Telepresence Systems* (*ITP*) *Version 3.0.3*:
  - RPX 200
  - RPX 400
  - OTX 300
  - TPX HD 306
  - ATX HD 300
- *Polycom* video conferencing endpoints *Version 3.0.3*
  - 7000 HD Rev C
  - 8000 HD Rev B
  - 9006
  - 4500
- *Cisco TelePresence® System* (*CTS*) *Version 1.7*
  - *CTS 1000*
  - *CTS 3000*

TIP is supported by RMX 1500/2000/4000 systems with *MPMx* cards.

Conferences hosted on the MCU can include a mix of existing end points (that do not support *TIP)* and *CTS* endpoints.

TIP-enabled endpoints must support *TIP Version 7* or higher. Calls from endpoints supporting older versions of *TIP* will be rejected.

Deployment Architectures

The following multipoint topologies are given as examples. Actual deployments will depend on user requirements and available infrastructure:

- **Single company with Polycom and Cisco Infrastructure**
  — *CTS* and *Polycom Telepresence Rooms* in a corporate environment.
- **Company to company via Service Provider**
  — **Model 1:** Mixed *Polycom* and *Cisco* infrastructure at one of the companies, *Cisco* only infrastructure at the other.
  — **Model 2:** *Polycom* only infrastructure at one of the companies, *Cisco* only infrastructure at the other.

Single Company Model - Polycom and Cisco Infrastructure

The deployment architecture in *Figure I-1* shows a company that has a mixture of *Polycom* and *Cisco* endpoints, room systems and telephony equipment that needs to enable multipoint calls between all its video and audio endpoints using the MCU as the conference bridge.

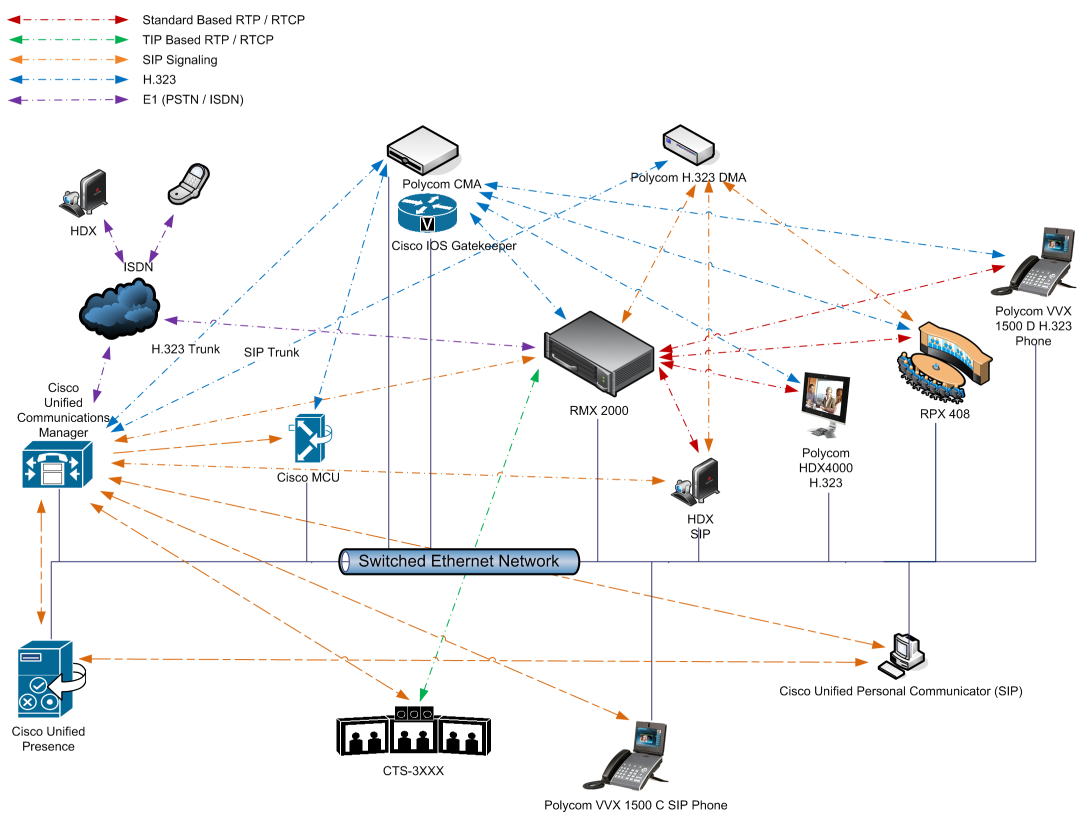


Figure I-1 *Single company with Polycom and Cisco Infrastructure*

The following table lists components and versions of the *MCU and Cisco Telepresence Systems (CTS) Integration Solution Architecture*.

Table I-1 *Solution Architecture Components*

Component	Version	Description
CISCO Equipment		
CUCM	8.5.1, 8.6.2	Cisco Unified Communication Manager: CUCM must be configured to: • Route calls to DMA (if present). • Route all H.323 calls to the gatekeeper, which can be either CMA or IOS.
IOS	15.1T	Cisco Internetwork Operating System - Gatekeeper
Endpoints (CTS)	1.7.2 (ATT), 1.8.1	Telephony, desktop and room systems. • *CTS* endpoints must register to *CUCM.*
Cisco Unified Video Conferencing 5230	7.2	MCU.
Cisco Unified Presence	8.5, 8.6	Network-based Presence and Instant Messaging.
Cisco Unified Contact Center Express	8.0, 8.5	Call distributor (ACD), interactive voice response (IVR) and computer telephony integration (CTI).
Cisco IP Communicator	7.0,8.6	Windows PC-based softphone application.
Cisco Unified Personal Communicator	8.5(2),8.5(5)	Web client for Presence and Instant Messaging.
Cisco Unified Video Advantage	2.2(2)	Video telephony functionality for Cisco Unified IP phones.
Cisco Unified IP Phones 7960, 7961, 7962, 7965, 7975	CUCM 8.5.1 / CUCM 8.6.1 compatible	IP Phones.
Cisco Unified IP Phones 9971	CUCM 8.5 / CUCM 8.6(2) compatible	
CTMS	1.7.3, 1.8.2	Cisco TelePresence Multipoint Switch.
Cisco Unified Border Element	15.1T	SBC - Voice and video connectivity from enterprise IP network to Service Provider SIP trunks.
Telepresence Server	2.2(1.54)	Telepresence Server.
VCS	X7.1	Video Communication Server / Session Manager.

Table I-1 *Solution Architecture Components*

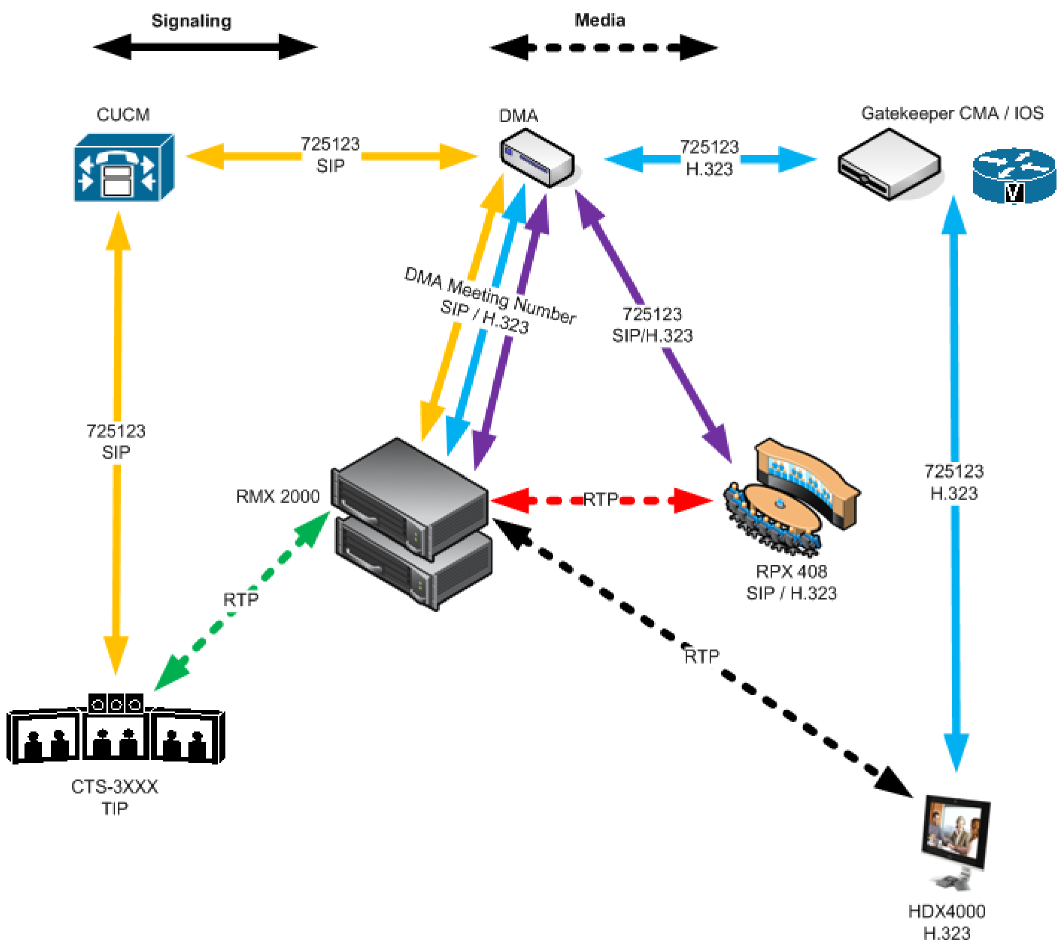
Component	Version	Description
Polycom Equipment		
DMA 7000	4.0	Polycom Distributed Media Application • *DMA* is an optional component but is essential if *Content* sharing is to be enabled. • All *SIP* endpoints register to *DMA* as a *SIP Proxy*. • DMA should be configured to route SIP calls (with CTS destination) to CUCM. If *DMA* is not present in the solution architecture, *SIP* endpoints must register to *CUCM* as gatekeeper. • *DMA* must be configured with a *VMR* (*Virtual Meeting Room*). Incoming calls are then routed to the MCU.
MCU	7.6 and higher	MCU: • Functions as the network bridge for multipoint calls between *H.323*, *SIP* and *TIP* endpoints. • The MCU can be interfaced to *CUCM* using a *SIP* trunk, enabling *CTS* to join multipoint calls on MCU. Signaling goes through the *CUCM* while the media in *TIP* format goes directly between the *CTS* and MCU. • The MCU must be configured to route outbound SIP calls to DMA. • The H.323 Network Service of the MCU should register it's dial prefix with the *CMA* gatekeeper. • When DMA is not used an *Ad-hoc Entry Queue*, designated as *Transit Entry Queue*, must be pre-defined on the MCU.
MLA	3.0.3	Multipoint Layout Application Required for managing multi-screen endpoint layouts for *Cisco CTS 3XXX, Polycom TPX*, *RPX* or *OTX* systems.
CMA	5.5	Polycom Converged Management Application - Gatekeeper • The gatekeeper must route calls to MCU based on the MCU prefix registration on the gatekeeper.
Endpoints		Telephony, desktop and room systems. • H.323 endpoints must register to the *CMA* or *IOS* gatekeeper. • *Polycom SIP* endpoints must register to *DMA* as *SIP Proxy* when *DMA* is used. • *H.323* endpoints must register to the *CMA* or *IOS* gatekeeper.

Call Flows

Multipoint call with DMA

In this example:

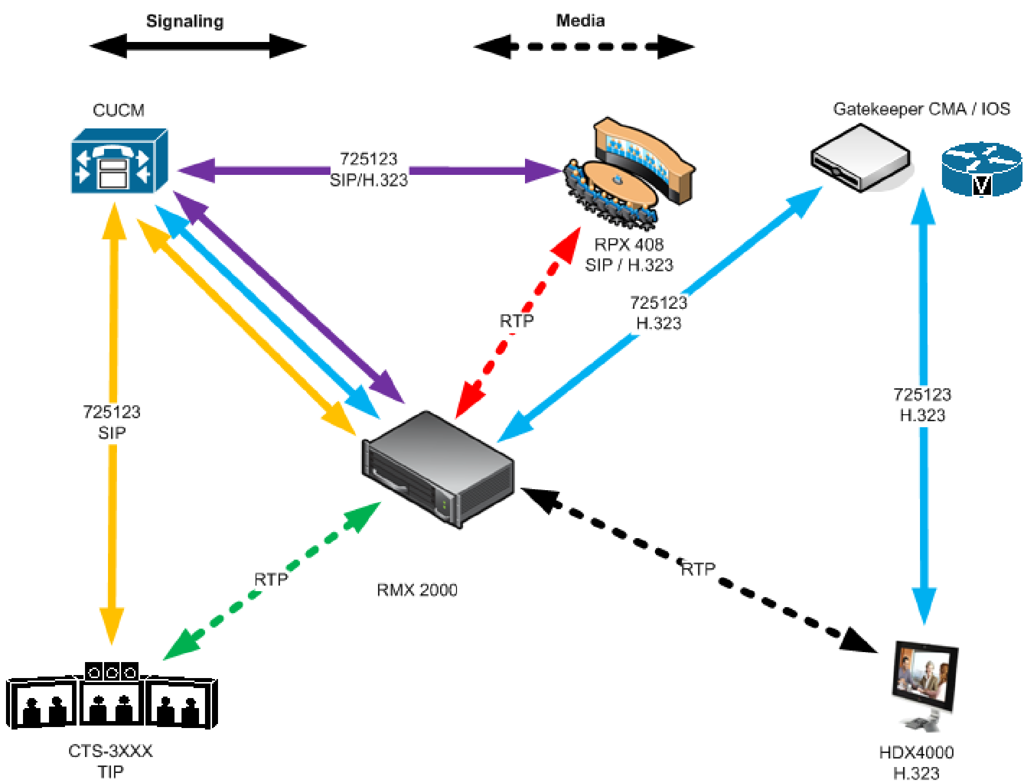
- MCU prefix in the gatekeeper 72
- *Virtual Meeting Room* in *DMA* 725123
- *DMA Meeting Number* Generated by *DMA*



Multipoint call without DMA

In this example:

- MCU prefix in the gatekeeper 72
- *CUCM* According to its *Dial Plan* forwards calls with prefix 72 to the *MCU*



Company to Company Models Using a Service Provider

Using this topology, both companies connect to a *Service Provider* via a *Cisco Session Border Controller* (*SBC)*. The *Service Provider* functions as a *B2B Telepresence Exchange,* enabling multipoint calls between the two companies and their respective video and audio endpoints using the MCU as the conference bridge.

The *SBC* functions as a firewall that the *Service Provider* can configure according to *Trust Relationships* between two or several companies. By using this method, companies do not have to open their corporate firewalls and administer connectivity with the many companies they may need to communicate with.

Two topology models are discussed:

- **Model 1:**
  - *Company A* has a *Polycom* only environment.
  - *Company B* has a *Cisco* only Environment.
- **Model 2:**
  - *Company A* has a mixed *Polycom* and *Cisco* environment.
  - *Company B* has a *Cisco* only Environment.

Model 1

The deployment architecture in *Figure I-2* shows two companies: *Company A* and *Company B*.

Company A - has deployed a *Polycom* solution including:

- *DMA*
- *MCU*
- *MLA*
- *CMA Gatekeeper*
- *Polycom* telephony and desktop endpoints.

The roles of the *Polycom* components are described in the *Polycom Equipment* section of Table I-1 on page **I-3**.

Company B - has deployed a *Cisco* solution including:

- CTS 1000
- CTS 3000
- *Cisco* telephony and desktop endpoints

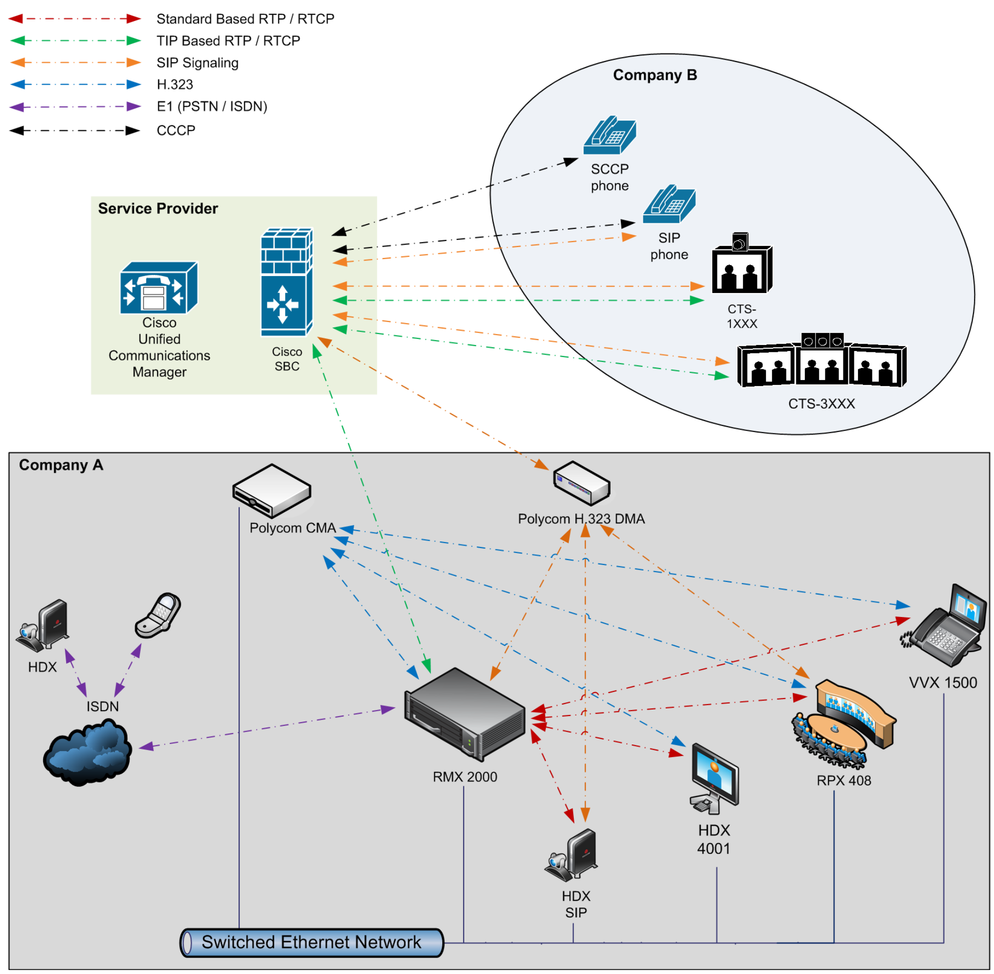


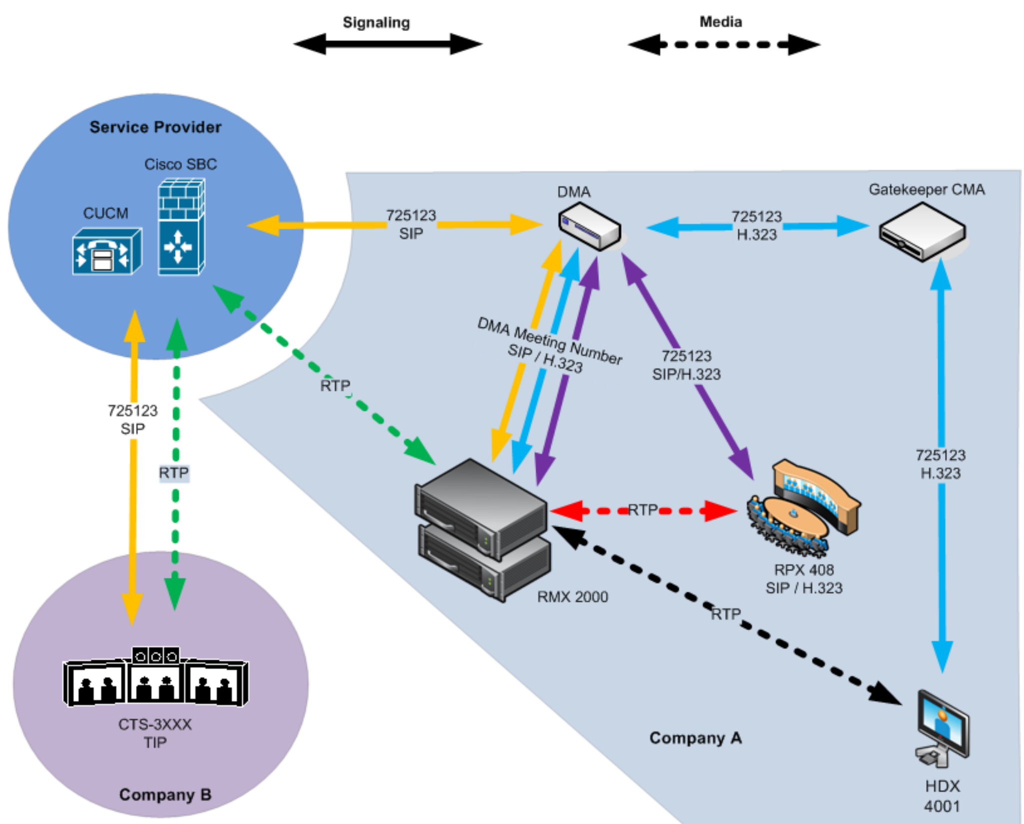
***Figure I-2** Company to Company via Service Provider - Model 1*

Call Flow

Multipoint call via Service Provider - Model 1

In this example:

- MCU prefix in the gatekeeper 72
- *Virtual Meeting Room* in *DMA* 725123
- *DMA Meeting Number* Generated by *DMA*



Model 2

The deployment architecture in *Figure I-3* shows two companies: *Company A* and *Company B*.

Company A - has the same deployment architecture as shown in "*Single Company Model - Polycom and Cisco Infrastructure"* on page **I-2**.

Company B - has deployed a *Cisco* solution including:

- CTS 1000
- CTS 3000
- *Cisco* telephony endpoints.

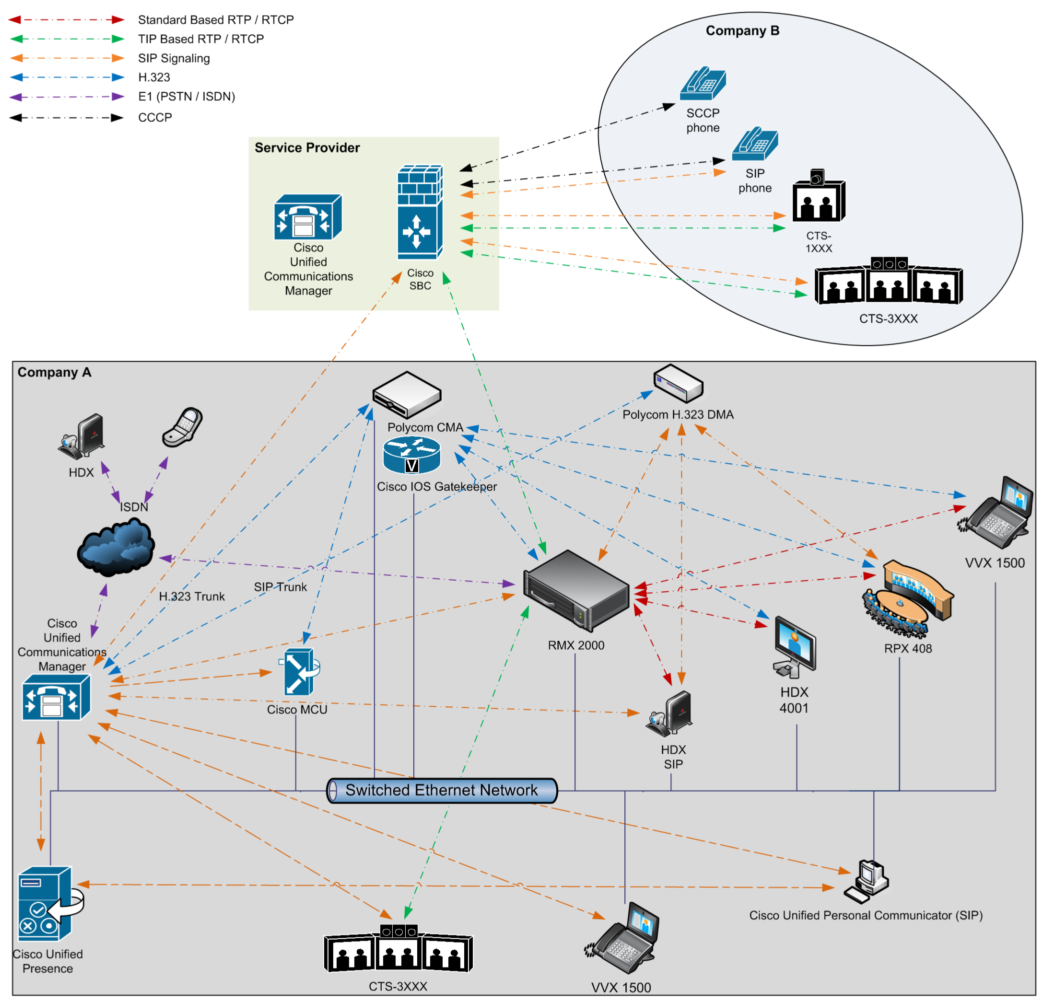


Figure I-3 *Company to Company via Service Provider - Model 2*

The deployment architecture includes:

Company A

For a full description of *Company A's* deployment, see "*Single Company Model - Polycom and Cisco Infrastructure"* on page **I-2**.

Differing or additional configuration requirements for each element of this deployment model are listed below:

Table I-2 *Solution Architecture Components*

Component	Version	Description
CISCO Equipment		
CUCM	8.5	Cisco Unified Communication Manager: CUCM must be configured with a SIP trunk to the Service Provider's SBC.
Polycom Equipment		
MCU	7.6.x	MCU: MCU must be configured to send and receive RTP streams to and from the Service Provider's SBC.

Company B

Table I-3 *Solution Architecture Components*

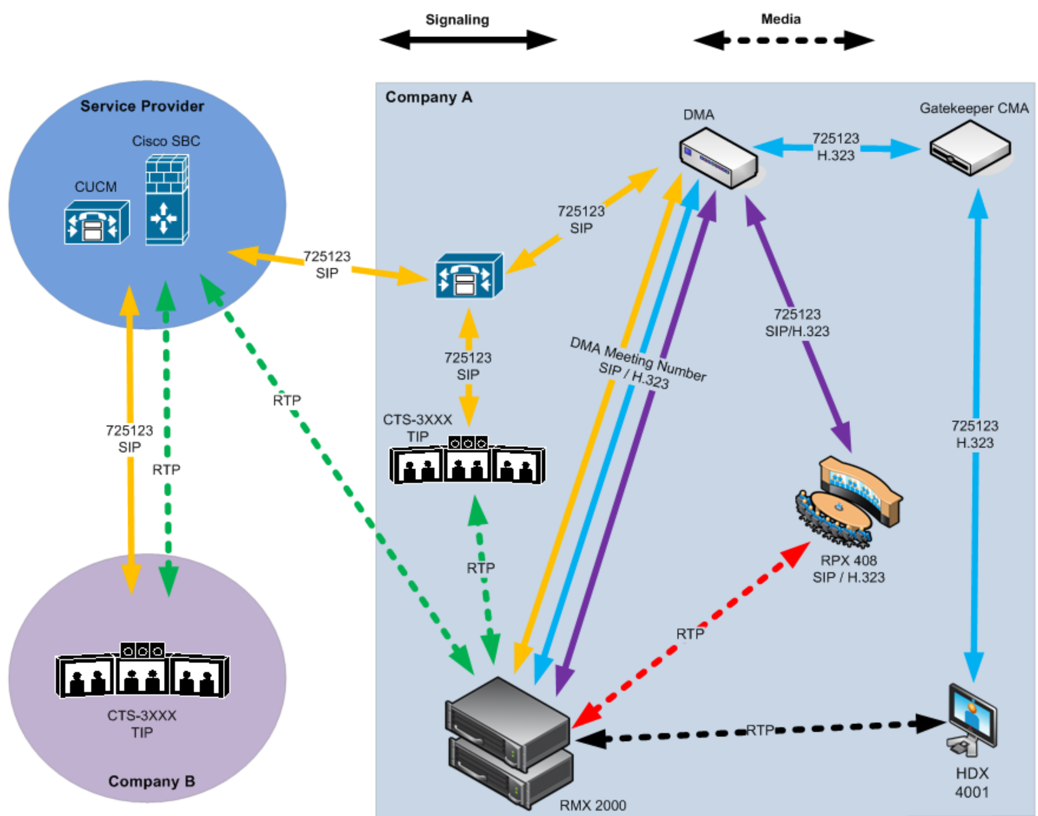
Component	Version	Description
CISCO Equipment		
Endpoints		Endpoints should register with the *Service Provider's CUCM* (or the local CUCM, if present).

Call Flow

Multipoint call via Service Provider - Model 2

In this example:

- *MCU* prefix in the gatekeeper — 72
- *Virtual Meeting Room* in *DMA* — 725123
- *CUCM* — According to its *Dial Plan* forwards calls with prefix 72 to the *MCU*



Administration

The various deployment combinations and settings within the various *Deployment Architectures* affects the administration of the system.

Gatekeepers

Standalone Polycom CMA System as a Gatekeeper

The *Polycom CMA* system can be used as the only gatekeeper for the network. Bandwidth and call admission control of endpoints registered with the *CMA* system is split between the *CMA* system and the *CUCM*.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Using a Polycom CMA System as a Gatekeeper*".

Standalone Cisco IOS Gatekeeper

The *Cisco IOS Gatekeeper* can be used as the only gatekeeper for the network if the management capabilities of the *Polycom CMA* system are not required.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Using a Standalone Cisco IOS Gatekeeper*".

Neighbored Cisco IOS and Polycom CMA Gatekeepers

Neighbored gatekeepers make it easier to create a common dial plan and should be considered when integrating an existing *Cisco* telephony environment with an existing *Polycom* network. *Neighbored Gatekeepers* allow number translation while maintaining the existing environments.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Neighbored Cisco IOS and Polycom CMA Gatekeepers*".

DMA

The *Polycom DMA* system can be configured as a *SIP* proxy and registrar for the environment. When used as a *SIP* peer, the *DMA* system can host video calls between *Cisco* endpoints that are registered with the *CUCM* and *Polycom SIP* endpoints that are registered with the *DMA* system.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Using a Polycom DMA System as SIP Peer*".

CUCM

When *Polycom SIP* endpoints (voice and video) are registered directly with *CUCM* you can take advantage of supported telephone functions. *CUCM* may not support the full range of codecs and features available on the *Polycom* equipment. *CUCM* supported codecs and features will be used in such cases.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager Participants*".

Configuring the Cisco and Polycom Equipment

MLA (*Multipoint Layout Application*) is required for managing *CTS 3XXX* layouts whether *Polycom TPX, RPX* or *OTX* systems are deployed or not. *MLA* is a *Windows®* application that allows conference administrators to configure and control video layouts for multipoint calls involving *Polycom Immersive Telepresence* (*ITP*) systems.

Call Detail Records (*CDR*) are generated on both the *CMA Gatekeeper* and the *CUCM* for reporting and billing purposes.

Content

Polycom and *Cisco* endpoints can share *Content* within a *Cisco TelePresence* environment. The content sharing experience depends on whether the endpoints are registered with the *DMA* or *CUCM*.

Table I-4 Endpoint Registration Options - Content Sharing Experience

Multipoint Calls on MCU	Content Sharing	People + Content
Endpoints Registered to DMA		
HDX/ITP to HDX/ITP	Yes	Yes
HDX/ITP to Cisco CTS	Yes	No
Cisco CTS to HDX/ITP	Yes	Yes
Endpoints Registered to CUCM		
HDX/ITP to HDX/ITP	Yes	No
HDX/ITP to Cisco CTS	Yes	No,
Cisco CTS to HDX/ITP	No	No

- *H.239*
  - — A variety of resolutions and frame rates are supported.
    For more information see "*H.239 / People+Content"* on page **4-1**.
  - — Can be used with *SIP* and *H.323* endpoints, desktop (*CMAD*), room systems (*HDX*) and *ITP* (*OTX, RPX*).
  - — Not supported by *Lync* clients, *IBM* clients and *Cisco CTS* endpoints.
  - — Cannot be used when *HDX* endpoints are registered to *CUCM.*
- *TIP*
  - — The resolution is fixed at XGA at 5fps.
  - — Supported on *HDX, Polycom ITP* and *Cisco CTS* systems.
- The following content compatibility options are available:
  - — **Tip not enabled** – *CTS* cannot join the conference, all other endpoints can share *H.239* content.
  - — **TIP video compatibility** – *CTS* receives people video, all other endpoints can share *H.239* content.
  - — **TIP video and content compatibility** – *CTS* and *HDX* can share *TIP* content, all other endpoints receive only the people video.

For more information see "*Procedure 4: Configuring a TIP Enabled Profile on the MCU*" on page **I-19**.

Cisco Equipment

To configure the various *Cisco* entities the following procedures are required.

CUCM

1 Configure the *CUCM* to send and receive calls from the *H*.323 network.

   a **With Neighbored IOS and CMA Gatekeepers**

   For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Configuring Cisco Unified Communications Manager for H.323*".

   b **With CMA Gatekeeper**

   For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Configuring Cisco Unified Communications Manager for H.323*".

   c **With IOS Gatekeeper**

   For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Configuring Cisco Unified Communications Manager for H.323*".

IOS Gatekeeper

>> Set up zones and gateway type prefixes to enable dialing to DMA and MCU systems.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Configuring the Cisco IOS Gatekeeper* ".

IOS and CMA Gatekeepers (Neighbored)

>> Configure the *Cisco IOS Gatekeeper* for two separate zones.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Configure the Cisco IOS Gatekeeper for use with a CMA System*".

Polycom Equipment

The following table lists the Polycom products supported within the various Deployment Architecture.

Only MCU configurations are described in detail in this document.

Configuration procedures for all other solution components are described in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Table I-5 *Supported current Polycom products*

Polycom TIP and SIP	Version(s)
Polycom DMA 7000 system	V4.0
Polycom RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000 systems	V7.6 and higher MPMx card is required.

Table I-5 Supported current Polycom products

Immersive Telepresence Systems: • RPX 200 and 400 systems • OTX 300 system • TPX HD 306 system • ATX HD 300 system	V3.0.3 Requires TIP option key. Requires Polycom Touch Control.
HDX Systems: • 7000 HD Rev C • 8000 HD Rev B • 9006 • 4500	V3.0.3 Requires TIP option key.
The following Polycom peripheral: • Polycom Touch Control	1.3.0
SIP ONLY (no TIP support)	**Version(s)**
Spectralink wireless phones 8020/8030	
Polycom VVX 1500	V4.0
Polycom VVX 1500 C	V3.3.1
KIRK Wireless Server 300/600v3/6000	

The following procedures **1** - **16** are a summary of the configuration procedures. The detailed procedures **1** - **16** begin with "*Procedure 1: Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag"* on page **I-17**.

MCU

1 Set the **MIN_TIP_COMPATIBILITY_LINE_RATE** *System Flag*
2 Configuring the MCU to statically route outbound *SIP* calls to *DMA* or *CUCM*
3 Configuring the MCU's *H.323 Network Service* to register with *CMA* gatekeeper
4 Configuring a *TIP* enabled *Profile* on the *MCU*
5 Configuring an *Ad Hoc Entry Queue* on the MCU if DMA is not used
6 Configuring a *Meeting Room* on the MCU
7 Configuring *Participant Properties* for dial out calls

DMA

If *DMA* is present in the configuration perform procedures **8** and **9**, otherwise skip to procedure **10**.

8 Configuring *DMA* to route *SIP* calls to *CUCM*
9 Configuring a *Virtual Meeting Room* (*VMR*)

The procedures for configuring *DMA* are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments.*

CMA

10 Configuring *CMA* to route *H.323* calls to MCU
11 Configuring *CMA* for use with *Cisco IOS Gatekeeper (Neighbored)*

12 Configuring *CMA* to route *H.323* calls to *CUCM*

13 Configuring *CMA* to route *non-H.323* calls to *CUCM*

The procedures for configuring *CMA* are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Endpoints

14 Configuring *H.323* endpoints to register to the CMA or IOS gatekeeper

The procedures for configuring *H.323* endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

15 Configuring *SIP* endpoints to register to:

a *DMA* as *SIP Proxy*

b *CUCM* as *SIP Proxy*

The procedures for configuring *SIP* endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

16 Configuring *TIP* endpoints to register to:

a *DMA*

b *CUCM*

The procedures for configuring *TIP- enabled* endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments.*

Procedure 1: Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag

The **MIN_TIP_COMPATIBILITY_LINE_RATE** *System Flag* determines the minimum line rate at which an *Entry Queue* or *Meeting Room* can be *TIP* enabled.

CTS version 7 requires a minimum line rate of 1024 kbps and will reject calls at lower line rates, therefore the *System Flag* value must be **1024** or higher.

For more information see "*Modifying System Flags"* on page **22-1**.

Procedure 2: Configuring MCU to statically route outbound SIP calls to DMA or CUCM

1 In the *IP Network Services Properties* dialog box, click the **SIP Servers** tab.

2 In the *SIP Server* field, select **Specify**.

3 In the *SIP Server Type* field, select **Generic**.

4 Set *Refresh Registration every* **3600** *seconds*.

5 If not selected by default, change the *Transport Type* to **TCP**.

6 In the *SIP Servers* table:

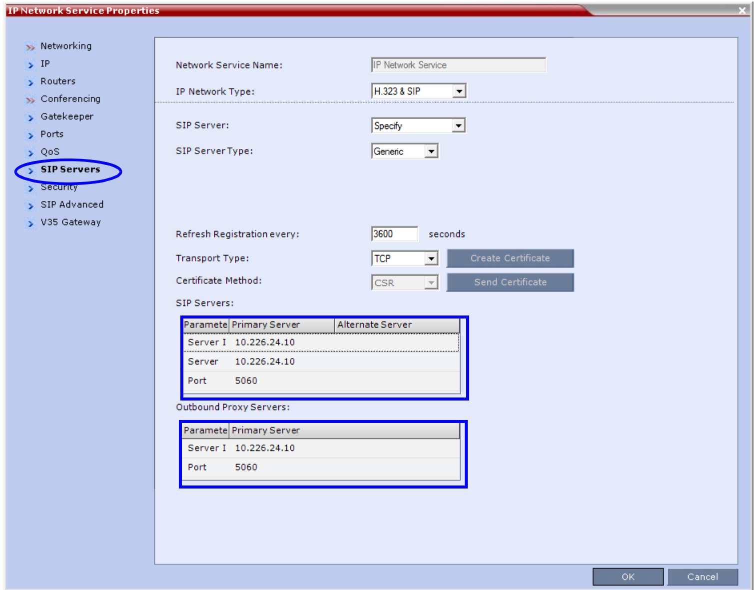
a Enter the *IP* address of the *DMA* or *CUCM* in both the *Server IP Address or Name* and *Server Domain Name* fields.

b The *Port* field must be set to it's default value: **5060**. *DMA* and *CUCM* use this port number by default.

7 In the *Outbound Proxy Servers* table:

a Enter the *IP* address in the *Server IP Address or Name* field. (The same value as entered in Step 6a.)

b The *Port* field must be set to it's default value: **5060**.
(By default, the *Outbound Proxy Server* is the same as the *SIP Server*.)

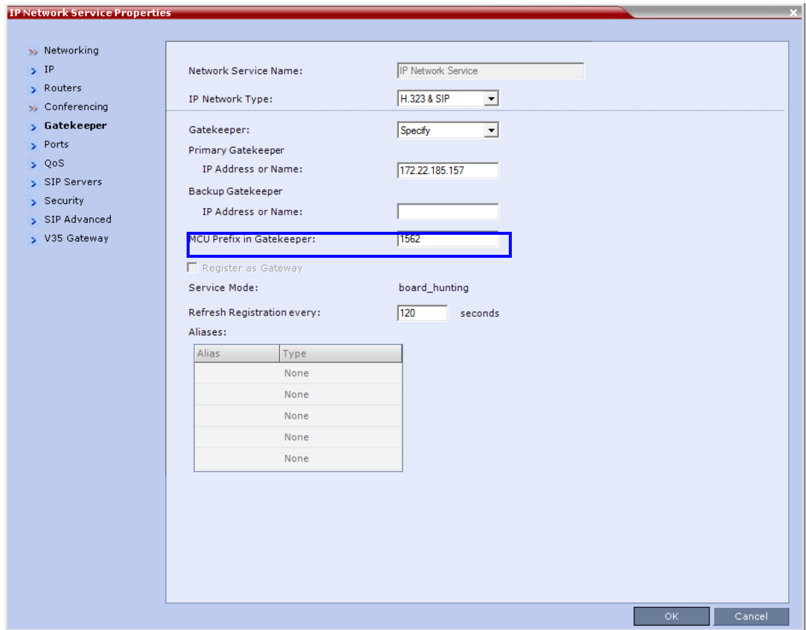


When configuring MCU to statically route *SIP* calls to *DMA* or *CUCM*, it is important to also configure the MCU's *H.323 Network Service* to register with *CMA* gatekeeper. For more information see "*Procedure 3: Configuring the MCU's H.323 Network Service to register with CMA gatekeeper"* on page **I-18**.

Procedure 3: Configuring the MCU's H.323 Network Service to register with CMA gatekeeper

1 In the *IP Network Services Properties* dialog box, click the **Gatekeeper** tab.

2 In the *MCU Prefix in Gatekeeper* field, enter the prefix that the MCU uses to register with the gatekeeper.

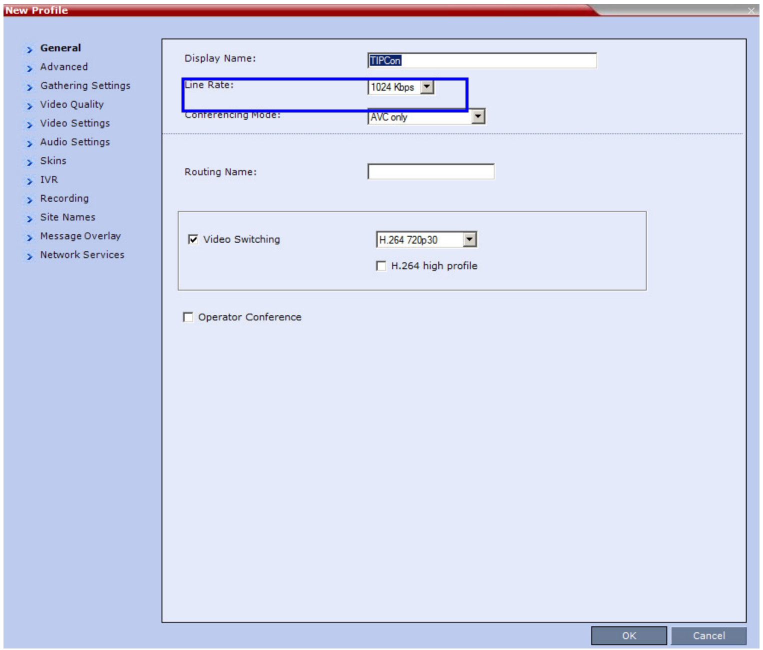


Procedure 4: Configuring a TIP Enabled Profile on the MCU

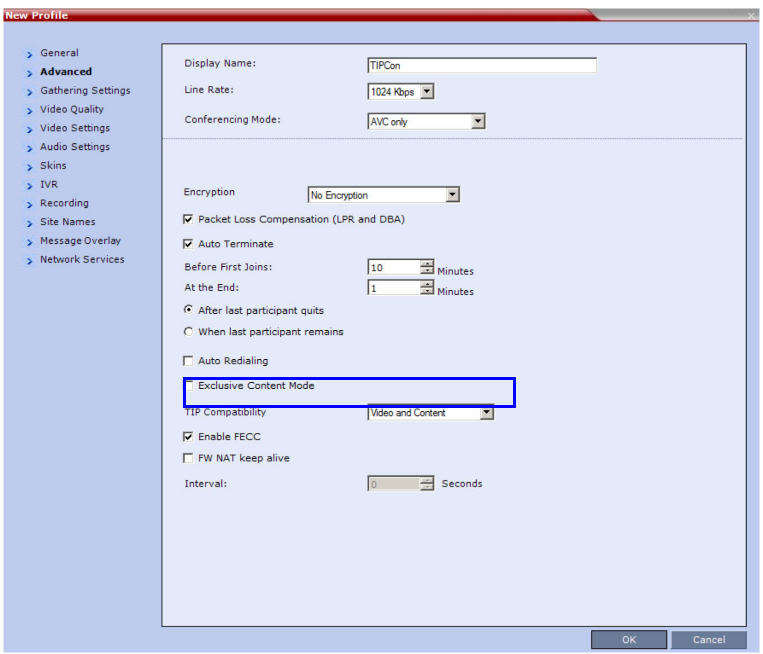
TIP enabled profiles must be used for the *Entry Queues* and *Meeting Rooms* defined on the MCU. (Different *Profiles* can be assigned to *Entry Queues* and *Meeting Rooms,* however they must be *TIP* enabled.)

1 Create a *New Profile* for the *Meeting Room*. For more information see "*Defining a CP Conference Profile"* on page **2-11**.

2 In the *New Profile - General* tab, set the *Line Rate* to a value of at least that specified for the **MIN_TIP_COMPATIBILITY_LINE_RATE** *System Flag* in *Procedure 1*.



3 Click the *Advanced* tab.



4 Select the *TIP Compatibility* mode: **Video and Content** is recommended.

Tables 10, 11 and 12 list the system's *Content* sharing behavior for the various combinations of *TIP Compatibility* mode settings and the following endpoints:

Polycom Immersive Telepresence Systems (*ITP*) *Version 3.0.3*:

- RPX 200
- RPX 400
- OTX 300
- TPX HD 306
- ATX HD 300

Polycom video conferencing endpoints (*HDX*) *Version 3.0.3*

- 7000 HD Rev C
- 8000 HD Rev B
- 9006
- 4500

Cisco TelePresence® System (*CTS*) *Versions 1.7 / 1.8*

- CTS 1000
- CTS 3000

Table 10 *TIP Compatibility - None*

None		Content Receiver	
		HDX / ITP	CTS
Content Sender	HDX / ITP	H.239 People+Content	Not Connected
	CTS	Not Connected	Not Connected

Table 11 *TIP Compatibility - Video Only*

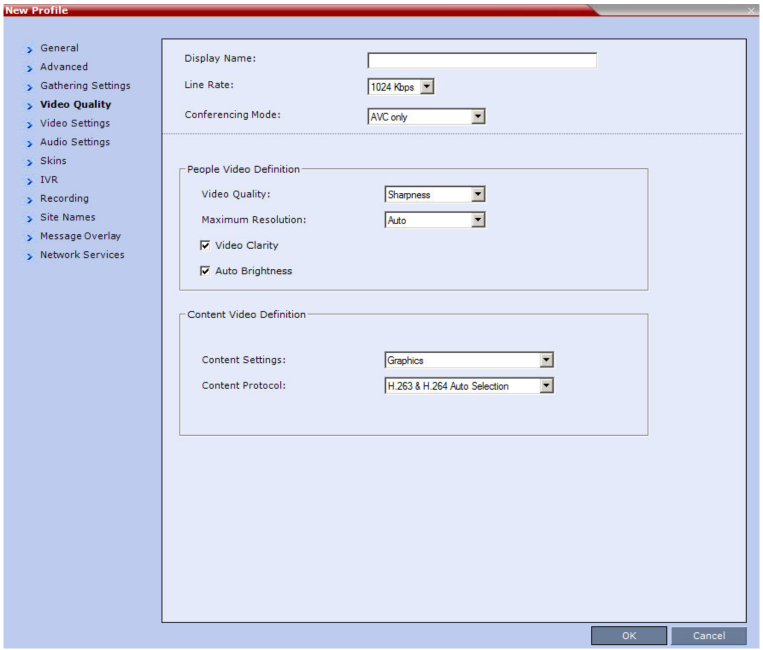
Video Only		Content Receiver	
		HDX / ITP	CTS
Content Sender	HDX / ITP	H.239 People+Content	None
	CTS	None	None

Table 12 *TIP Compatibility - Video & Content*

Video & Content		Content Receiver	
		HDX / ITP	CTS
Content Sender	HDX / ITP	H.239	TIP Content
	CTS	TIP Content	TIP Content

Selecting *TIP Compatibility* as **Video and Content** disables *Content Settings* in the *Video Quality* tab.

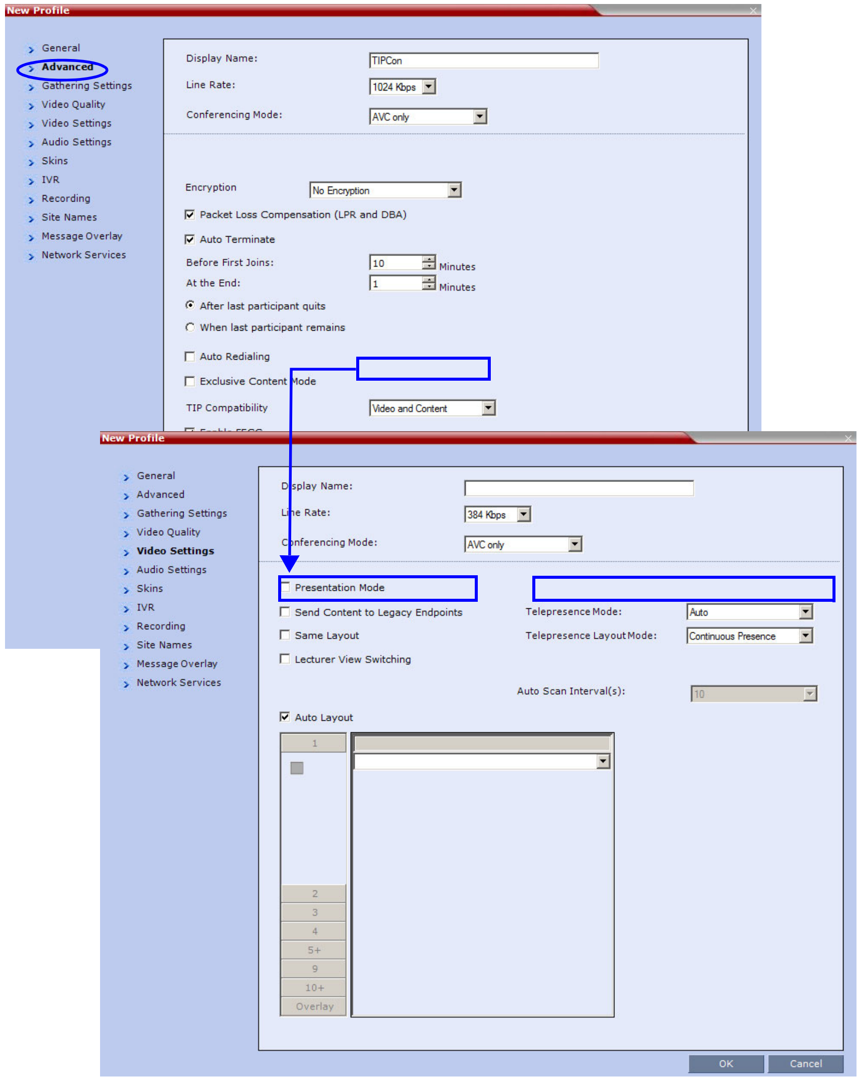
5 Click the *Video Quality* tab.



Content Settings is disabled if *TIP Compatibility* is set to **Video and Content** in the *Advanced* tab.

6 Click the *Video Settings* tab.

If the *TIP Compatibility Mode* was set to **Video and Content**, the *Send Content to Legacy Endpoints* disabled. This setting cannot be changed.



7 Set the *Telepresence Mode* to **Auto**.

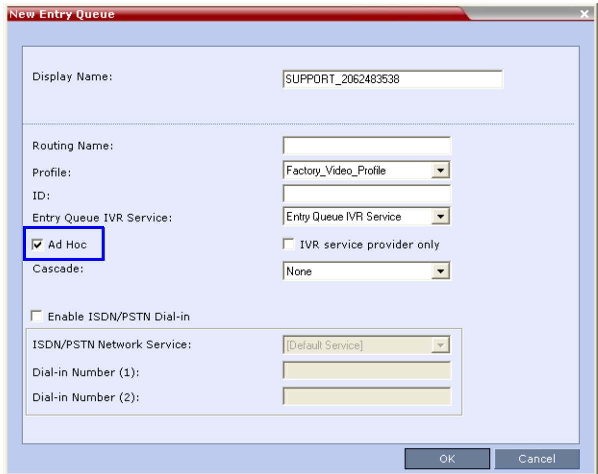
8 Assign the *New Profile* to the *Meeting Room*. For more information see "*Creating a New Meeting Room"* on page 6-4.

Procedure 5: Configuring an Ad Hoc Entry Queue on the MCU if DMA is not used

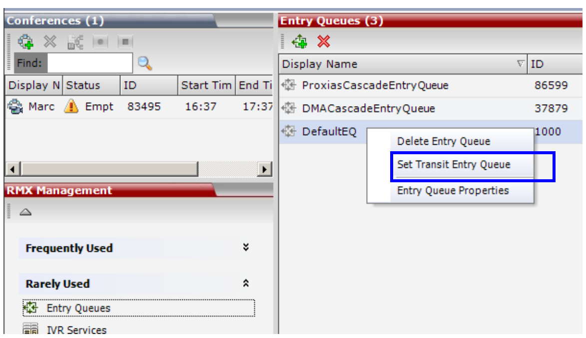
You must discuss the selection of the appropriate Profile for this EQ, as this Profile will be used to create the conferences on the MCU and they must be TIP enabled.

1 Create or select the *Entry Queue* as described in "*Entry Queues"* on page 7-1.

2 In the *New Entry Queue* or *Entry Queue* Properties dialog box, ensure that **Ad Hoc** is selected.



3 Ensure that the *Entry Queue* is designated as the **Transit Entry Queue** as described in "*Setting a Transit Entry Queue"* on page **7-6**.



Procedure 6: Configuring a Meeting Room on the MCU

The *Profile* for the *Meeting Room* must be *TIP* enabled as described in *Procedure 4*.

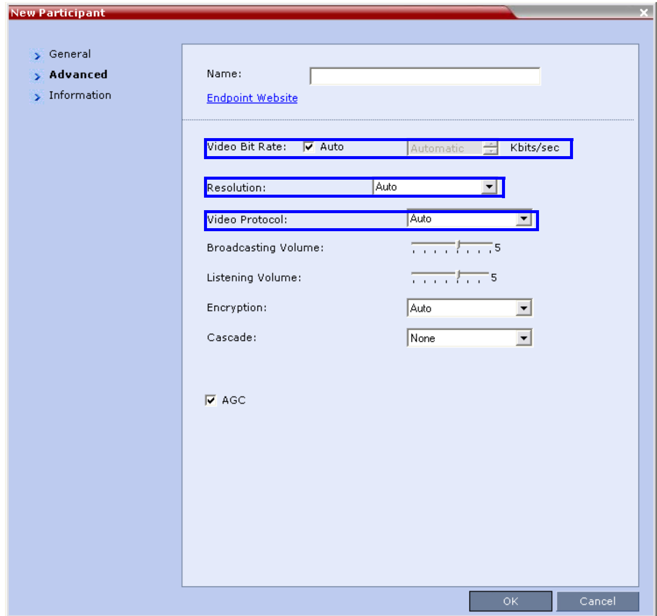
For more information see "*Creating a New Meeting Room"* on page **6-4**.

Procedure 7: Configuring Participant Properties for dial out calls

Participant Properties must be configured to ensure that defined participants inherit their *TIP* settings from the *Profile* assigned to the *Meeting Room*.

a Define the *New Participant's General* settings. For more information see "*Adding a Participant to the Address Book"* on page **8-8**.

b Click the *Advanced* tab.



c Ensure that:

- *Video Bit Rate* is set to **Automatic** or at least equal to or greater than the value specified by the **MIN_TIP_COMPATIBILITY_LINE_RATE** *System Flag*.
- *Resolution* is set to **Auto** or at least **HD 720**.
- *Video Protocol* is set to **Auto** or at least **H.264**.

Collaboration with Microsoft and Cisco

This solution enables *Polycom, Microsoft* and *Cisco* users, each within their own environment, to participate in the same conference running on an MCU.

The MCU natively inter-operates with *Microsoft Lync* and *Cisco TelePresence Systems*, ensuring optimum quality multi-screen, multipoint calls between:

- *Polycom Immersive Telepresence Systems* (*ITP*) *Version 3.0.3*:
  - — RPX 200
  - — RPX 400
  - — OTX 300
  - — TPX HD 306
  - — ATX HD 300
- *Polycom* video conferencing endpoints *Version 3.0.3*
  - — 7000 HD Rev C
  - — 8000 HD Rev B
  - — 9006
  - — 4500
- *Microsoft*
  - — *MS Lync* (using *MS-ICE*)
  - — *RTV 720p*

- *Cisco TelePresence® System* (*CTS*) *Versions 1.7 / 1.8*
  — *CTS 1300*
  — *CTS 3010*

Deployment Architecture

- *DMA* is required as all calls are dial-in to *Virtual Meeting Rooms* (*VMR*) provisioned on the *DMA*.
- *Microsoft* and *Cisco* clients dial the same *VMR* number to connect to the conference.
- Dial- out calls are not supported
- *Lync Clients* can not share content with *CTS*
- SIP trunks are required to the *DMA from:*
  — *MS Lync* as a *Static Route*.
  — *CUCM*

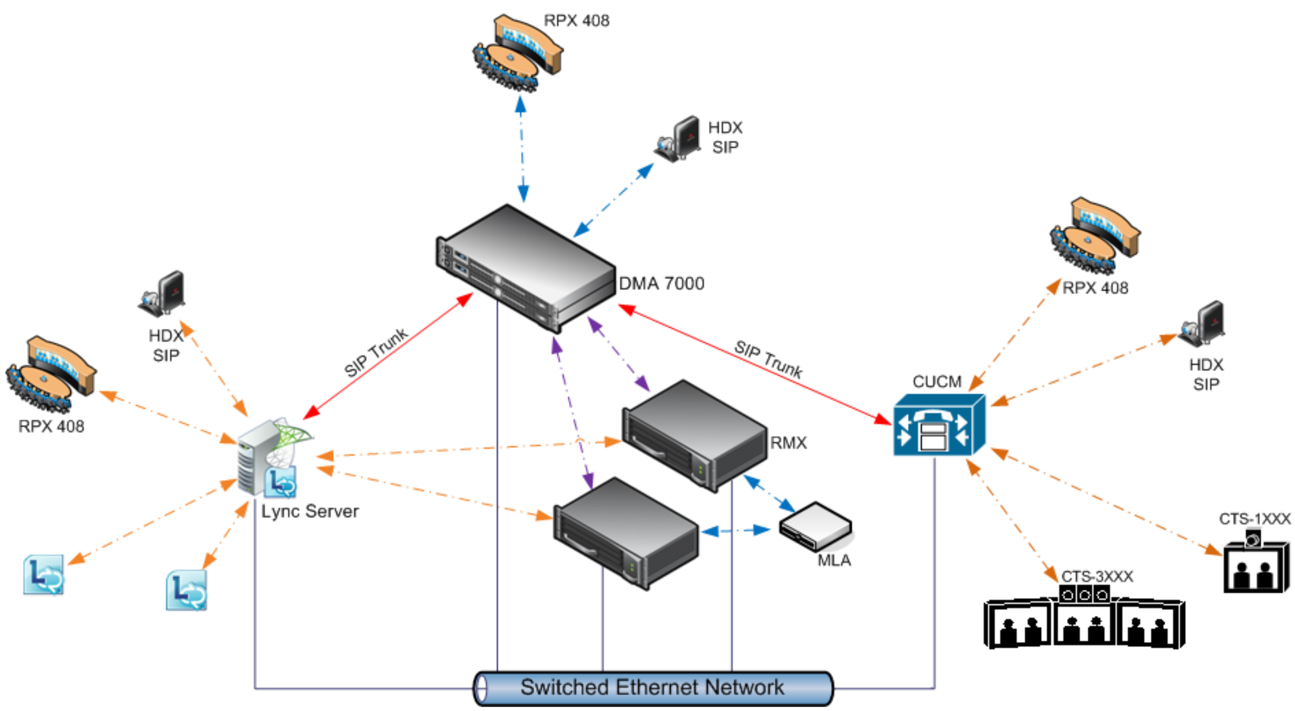


Figure I-4 *POCN Polycom, Microsoft and Cisco Infrastructure. Solution Architecture components.*

Component	Version
Polycom	
HDX	3.0.5
RSS	8.0
DMA	5.0

Component	Version
CMA	6.0.1
CMAD	5.2.3
ITP (OTX, RPX, ATX, TPX)	3.0.5
Conferencing for Outlook (PCO)	1.0.7
Touch Control	1.3
Microsoft	
OCS 2007 R2	3.5.6907.236
Lync 2010	4.0.7577.183 CU4
OC 2007 R2 client	3.5.6907.236
Lync 2010 client	4.0.7577.4051 CU4
Exchange 2007 R2 SP3	8.3.213.1
Exchange 2010 SP2	14.2.247.5
Outlook 2007	12.0.6557.5001 SP2
Outlook 2010	14.0.6112.5000
Cisco	
CUCM	8.5, 8.6.2
Cisco Unified Personal communicator	8.5(2),8.5(5)
Cisco Unified IP Phones 7960, 7961, 7962, 7965, 7975	CUCM 8.5 / CUCM 8.6(2) Compatible
CTS	1.7.4, 1.8.1
C90, C20	TC5.0

The following are not supported:

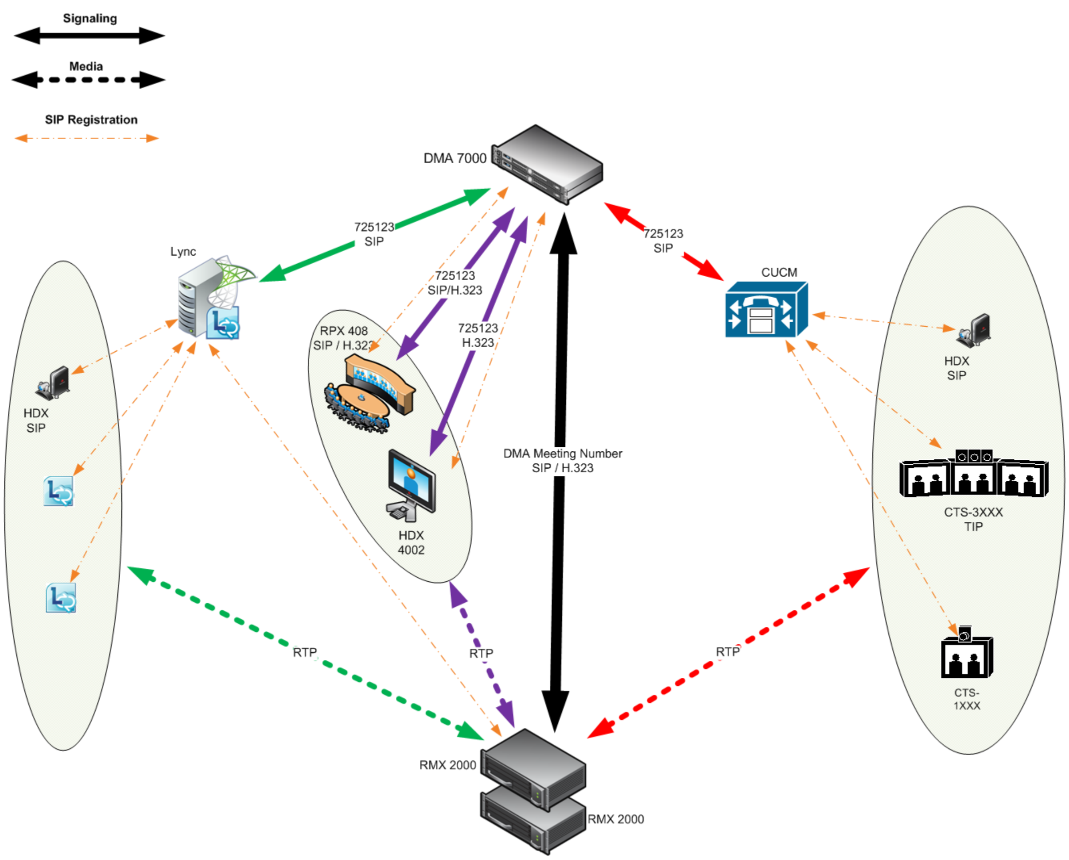
- In the *Lync* environment*:*
  - Sending or receiving *Content*.
  - Dial-out to *Lync* clients.
  - Presence of *VMRs*
- In the *Cisco* environment*:*
  - *TLS* and *SRTP*
  - *OBTP*

Call Flow

Multipoint Calls using DMA

In this example:

- Endpoint registration to either *DMA*, *Lync* or *CUCM.*
- *DMA* dial in *Prefix* 72
- *Virtual Meeting Room* in *DMA* 725123
- *DMA Meeting Number*Generated by *DMA*



Administration

The various deployment combinations and settings within the *Deployment Architecture* affects the administration of the system.

DMA

The *DMA* system can be configured as a *SIP* proxy and registrar for the environment as well as a *Gatekeeper* for dial in *H.323* calls. When configured as a *Gateway* for dial in *H.323* calls, it enables *H*.323 endpoints to connect to the same *VMR* as *SIP* clients.

When used as a *SIP* peer, the *DMA* system can host video calls between *Cisco* endpoints that are registered with the *CUCM, Lync Clients* that are registered with the *Lync Server* and *Polycom* endpoints that are registered with the *DMA* system.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Using a Polycom DMA System as SIP Peer*".

Microsoft Lync Server

Microsoft Lync Server manages *Presence* for each registered *Polycom* endpoint and enables video calls between *Lync Clients* and *Polycom* endpoints allowing *Lync* contacts to be called without needing to know their addresses.

RTV video, *MS-ICE* and *Lync*-hosted conferencing are supported when *Polycom* endpoints are registered to *Lync* Server. *Polycom* endpoints use *H.264*, while *Lync* Clients use the *RTV* protocol.

CUCM

When *Polycom SIP* endpoints (voice and video) are registered directly with *CUCM* you can take advantage of supported telephone functions. *CUCM* may not support the full range of codecs and features available on the *Polycom* equipment. *CUCM* supported codecs and features will be used in such cases.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager Participants*".

Configuring the Microsoft, Cisco and Polycom Components

1 Configure a *SIP Trunk* connection between the *Polycom DMA* system and the *Cisco Unified Communications Manager* (*CUCM*).

   For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Using a Polycom DMA System as SIP Peer*".

2 Register the MCU to the *Lync* Server

   a Install a *Security Certificate* on the MCU.

      The *Certificate* is obtained from the *System Administrator* and saved on the *Workstation*.

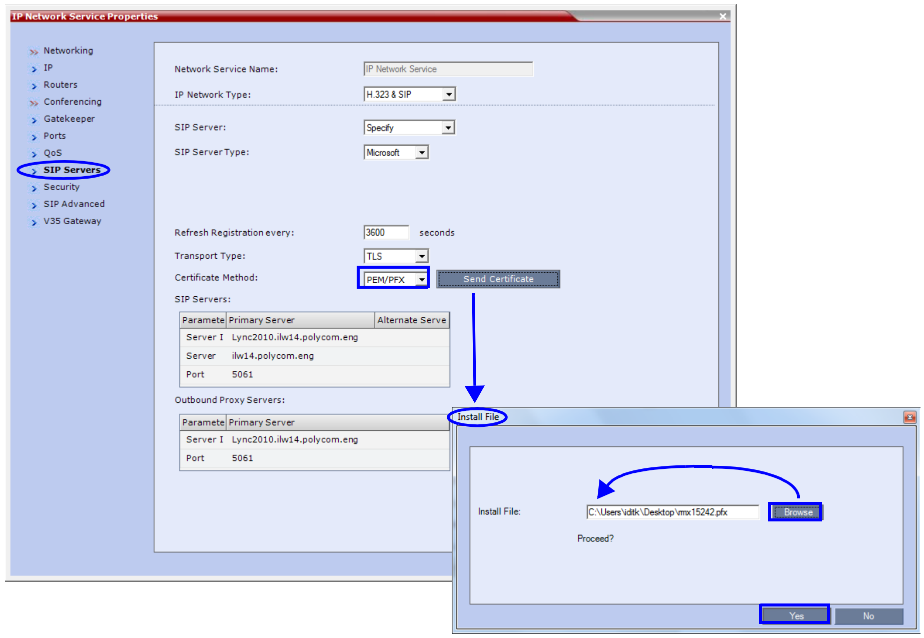
   b In the *SIP Servers* tab of the *IP Network Services Properties* dialog box:

      iIn the *Certificate Method* drop-down menu, select **PEM/PFX**.

      iiClick the **Send Certificate** button.

         The *Install File* dialog box is displayed.

iiiBrowse to the saved *Certificate* on the *Workstation* and click the **Yes** button to install the certificate.



For more information see:

- "*Setting the MCU for Integration Into Microsoft Environment”* on page **H-1**.
- *Polycom Unified Communications Deployment Guide for Microsoft Environments, “Configuring Your MCU System for use with the Lync Server”*.

3 Register the MCU with the *Lync Server*.

a In the *IP Network Services Properties* dialog box, click the **SIP Servers** tab.

b In the *SIP Server* field, select **Specify**.

c In the *SIP Server Type* field, select **Microsoft**.

d Set *Refresh Registration every* **3600** *seconds*.

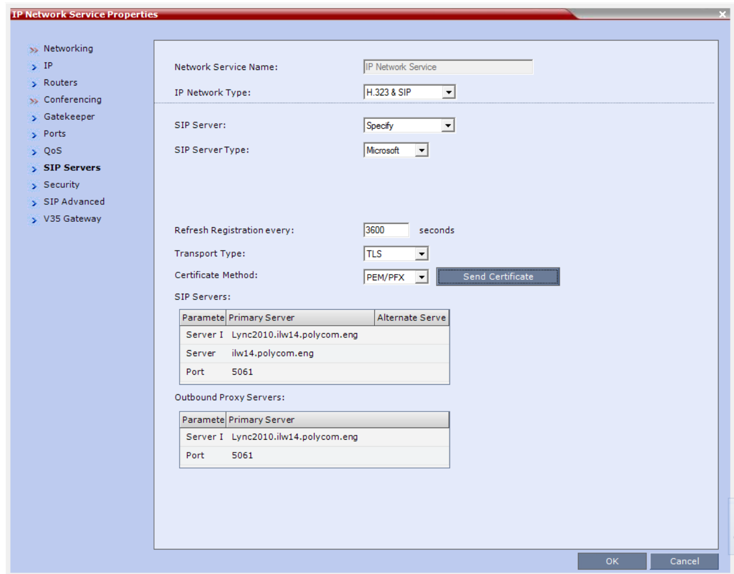
e If not selected by default, change the *Transport Type* to **TLS**.

f In the *SIP Servers* table, enter the *IP* address of the *Lync Server* in both the *Server IP Address or Name* and *Server Domain Name* fields.

g In the *SIP Servers* table, the *Port* field must be set to **5061**.

h In the *Outbound Proxy Servers* table, enter the *IP* address in the *Server IP Address or Name* field. (The same value as entered in Step f.)

i In the *Outbound Proxy Servers* table, the *Port* field must be set to **5061**. (The same value as entered in Step g.)



For more information see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

4 Set the **MIN_TIP_COMPATIBILITY_LINE_RATE** *System Flag*.

The **MIN_TIP_COMPATIBILITY_LINE_RATE** *System Flag* determines the minimum line rate at which a *Profile* can be *TIP* enabled.

CTS version 1.7 requires a minimum line rate of 1024 kbps and will reject calls at lower line rates, therefore the *System Flag* value must be **1024** or higher.

For more information see "*Modifying System Flags"* on page **22-1**.

5 Reset the MCU.

6 For more information see "*Resetting the RMX"* on page **21-69**.

7 Register the *DMA* to the *Lync* server

For more information see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*, *"Configure a DMA System SIP Peer for the Lync Server"*.

8 Register the *ITP* endpoints to the *Lync* server

For more information see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*, *"Deployment Process for Polycom Immersive Telepresence Systems"*.

9 Register *Lync Clients* to the *Lync* server

For more information see the relevant *Lync* documentation.

10 Register *DMA* to the *CUCUM* server

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, *"Using a Polycom DMA System in a Cisco Environment"*.

11 Register *CTS1000* and *CTS3000* endpoints to the *CUCUM* server

For more information see the relevant *Cisco* documentation.

12 Register *ITP* endpoints to the *CUCM* server.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, "*Direct Registration of Polycom Telepresence Systems with the Cisco Unified Communications Manager*".

13 Register *HDX* endpoints to the *DMA* as *Gatekeeper*

For more information see the *Polycom® DMA™ 7000 System Operations Guide*.

14 Open MLA to configure ITP Layouts

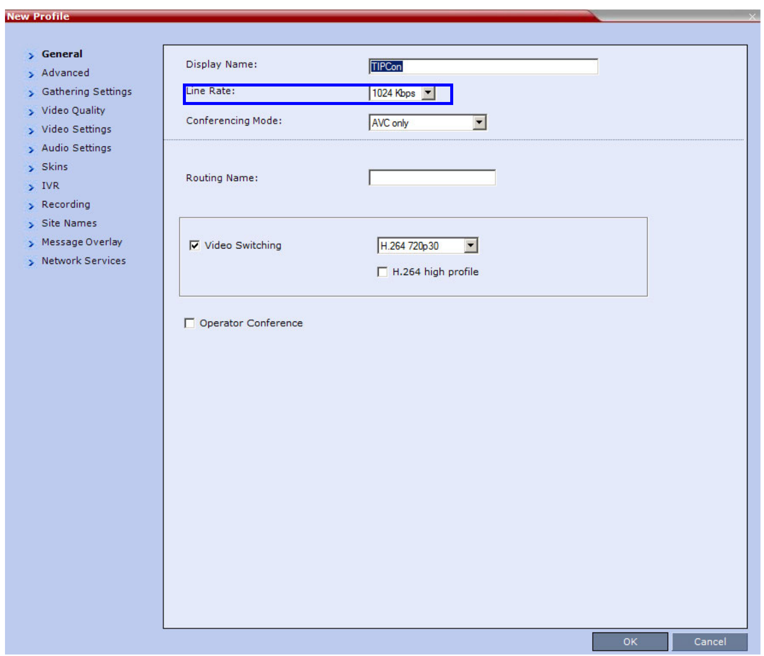
MLA (*Multipoint Layout Application*) is required for managing *CTS 3XXX* layouts whether *Polycom TPX, RPX* or *OTX* systems are deployed or not. *MLA* is a *Windows®* application that allows conference administrators to configure and control video layouts for multipoint calls involving *Polycom Immersive Telepresence* (*ITP*) systems.

For more information see *Polycom Multipoint Layout Application (MLA) User's Guide for Use with Polycom Telepresence Solutions*.

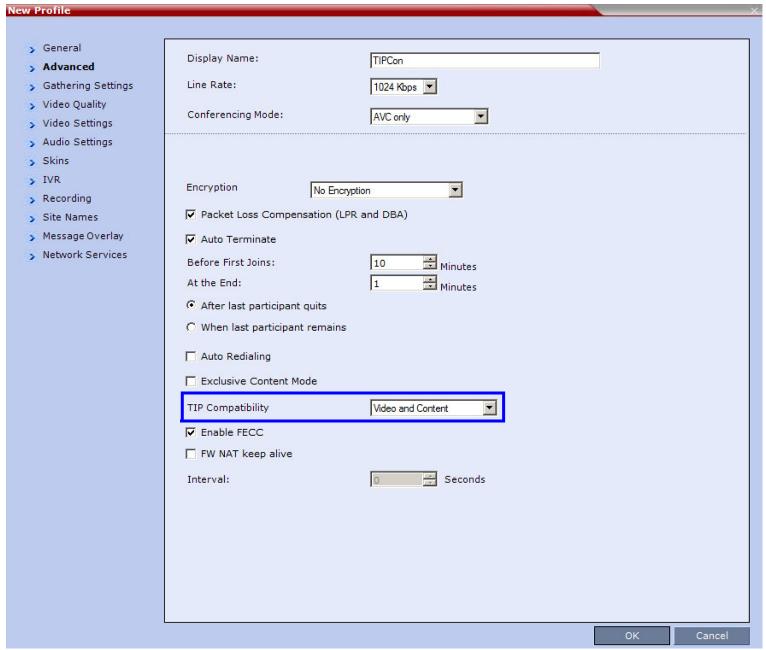
15 Configure a *TIP Enabled Profile* on the MCU.

a Create a *New Profile* for the *Meeting Room*.
For more information see "*Defining New Profiles*" on page **2-18**.

b In the *New Profile - General* tab, set the *Line Rate* to a value of at least that specified for the **MIN_TIP_COMPATIBILITY_LINE_RATE** *System Flag* in *Procedure 1*.



c Click the *Advanced* tab.



d Select the *TIP Compatibility* mode: **Video and Content** is recommended.

Tables I-1, I-2 and I-3 list the system's *Content* sharing behavior for the various combinations of *TIP Compatibility* mode settings and the following endpoints:

Polycom Immersive Telepresence Systems (*ITP*) *Version 3.0.3*:

- RPX 200
- RPX 400
- OTX 300
- TPX HD 306
- ATX HD 300

Polycom video conferencing endpoints (*HDX*) *Version 3.0.3*

- 7000 HD Rev C
- 8000 HD Rev B
- 9006
- 4500

Cisco TelePresence® System (*CTS*) *Versions 1.7 / 1.8*

- CTS 1300
- CTS 3010

Table I-1 *TIP Compatibility - None*

None		Content Receiver	
		HDX / ITP	**CTS**
Content Sender	**HDX / ITP**	H.239	Not Connected
	CTS	Not Connected	Not Connected

Table I-2 *TIP Compatibility - Video Only*

Video Only		Content Receiver	
		HDX / ITP	**CTS**
Content Sender	**HDX / ITP**	H.239	None
	CTS	None	None

Table I-3 *TIP Compatibility - Video & Content*

Video & Content		Content Receiver	
		HDX / ITP	**CTS**
Content Sender	**HDX / ITP**	H.239	TIP Content
	CTS	TIP Content	TIP Content

Selecting *TIP Compatibility* as **Video and Content** disables *Content Settings* in the *Video Quality* tab.

Encryption

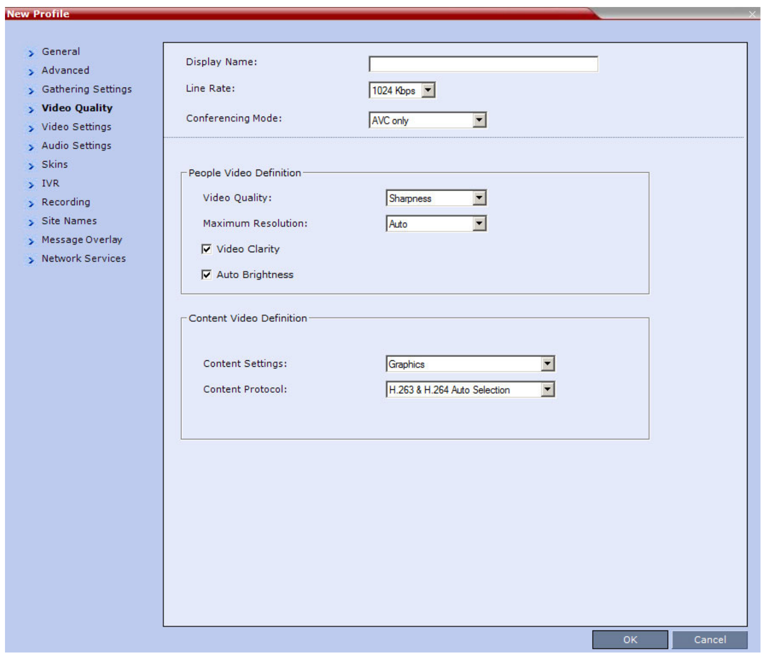
Set the encryption setting in the conference *Profile* to **Encrypt When Possible.**

Set the FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE *System Flag* to **NO**

These setting will enable encrypted and non-encrypted *H.323* participants to connect to encrypted or non-encrypted conferences.

For more information see *"Encryption"* on page 2-52.

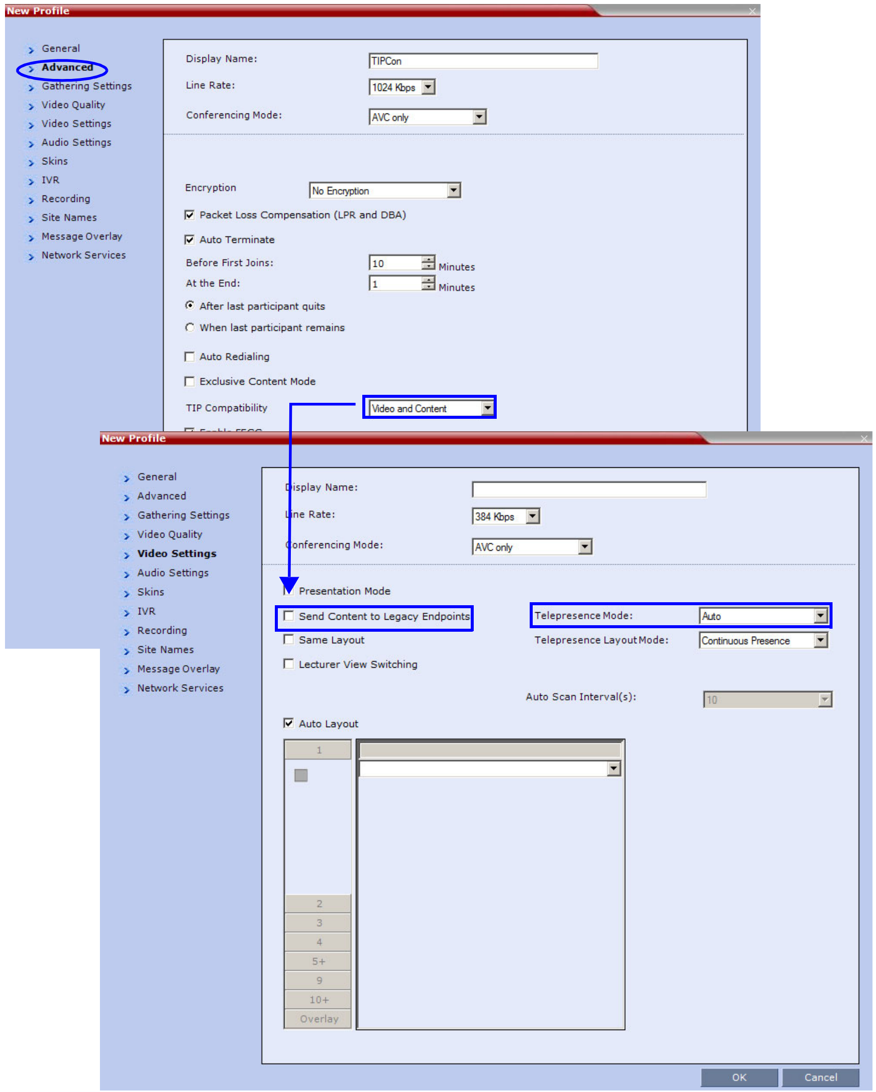
e Click the *Video Quality* tab.



Content Settings is disabled if *TIP Compatibility* is set to **Video and Content** in the *Advanced* tab.

f Click the *Video Settings* tab.

If the *TIP Compatibility Mode* was set to **Video and Content**, the *Send Content to Legacy Endpoints* disabled. This setting cannot be changed.



g Set the *Telepresence Mode* to **Auto**.

16 Configure a *Virtual Meeting Room* (*VMR*) on the *DMA*

The procedures for configuring *DMA* are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments.*

Endpoints

17 Configure *HDX* endpoints to register to *Lync Server.*

The procedures for configuring *HDX* endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

18 Configure *H.323* endpoints to register to *DMA* as *SIP Proxy*

The procedures for configuring *SIP* endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments.*

19 Configure *SIP* endpoints to register to:

- *DMA* as *SIP Proxy*
- *Lync Server* as *SIP Proxy*
- *CUCM* as *SIP Proxy*

The procedures for configuring *SIP* endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments.*

20 Configure *TIP* endpoints to register to:

- DMA
- CUCM

The procedures for configuring *TIP- enabled* endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments.*

Content

Endpoint Registration and *Dialing Method* affect the *Video* and *Content Sharing* characteristics of the conference as detailed in Table I-4.

Table I-4 *Video and Content*

Dialing Method	**Endpoint Registration**		
	Lync	**CUCM**	**DMA**
	ITP /HDX RTV Key is required for HDX and ITP	**ITP /HDX** TIP Key is required for HDX	**ITP /HDX** TIP Key is required for HDX
HDX to MCU	• HD H.264 Video • SIP P+C • Content: XGA,5fps • ICE	• HD H.264 Video • No Content • ICE not supported	• HD H.264 Video • SIP P+C • Content: XGA,5fps • ICE not supported
Lync to MCU	• HD Video (RTV) • No Content Sharing • Content sent to Lync using Content for Legacy Endpoints (Not supported in ITP Mode)		
CTS to MCU	• HD1080p30 • TIP Content Sharing • Content: XGA,5fps		

Operations During Ongoing Conferences

Moving participants between TIP enabled meetings and non TIP enabled meetings is not possible.

Monitoring

CTS Participants

1 In the *Participant List* pane double-click the participant entry. Alternatively, right-click a participant and then click **Participant Properties**.

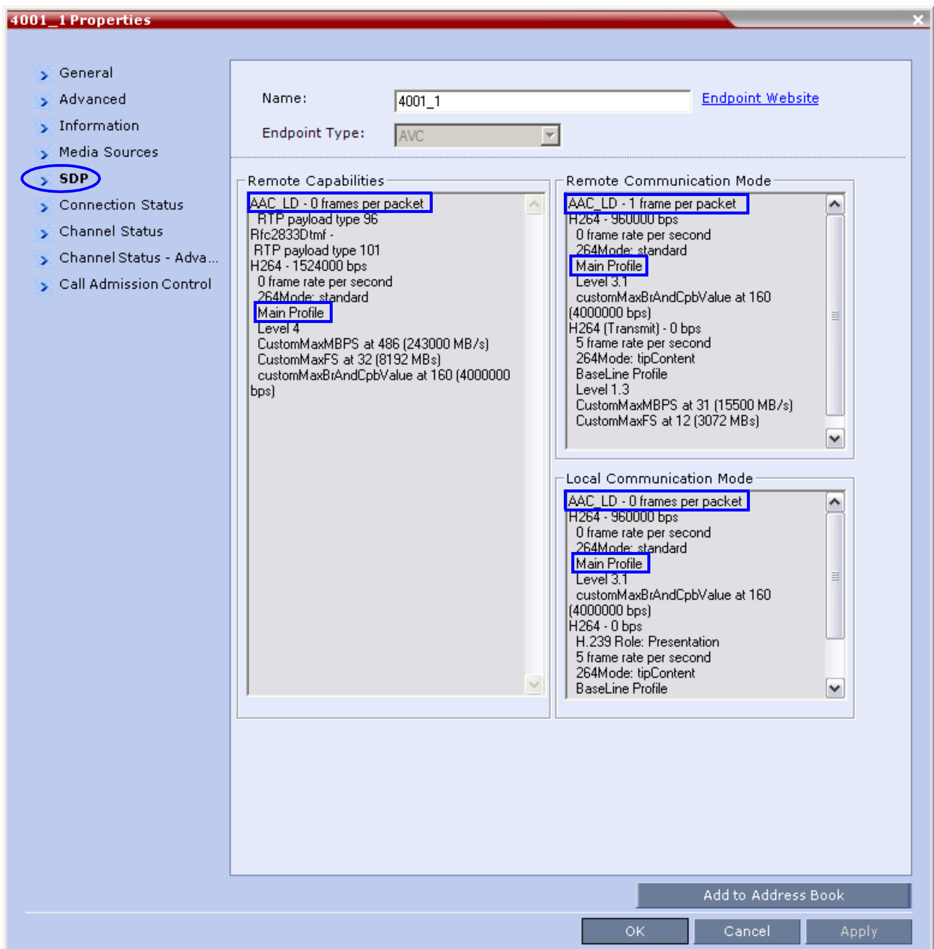
The *Participant Properties - General* dialog box opens.

2 Click the **SDP** tab.

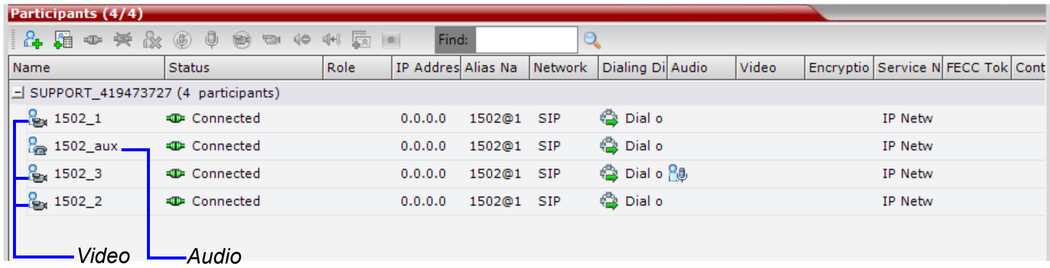
The following are indicated in the *Remote Capabilities*, *Remote Communication Mode* and *Local Communication Mode* panes:

— AAC_LD - Audio Protocol

— Main Profile - Video protocol



When viewing *CTS* systems in the *Participants* list, the individual video screens and the *Audio Channel* (*AUX*) of the *CTS* system are listed as separate participants. The *Participant* list below shows a connected *CTS 3000,* a 3-screen system.



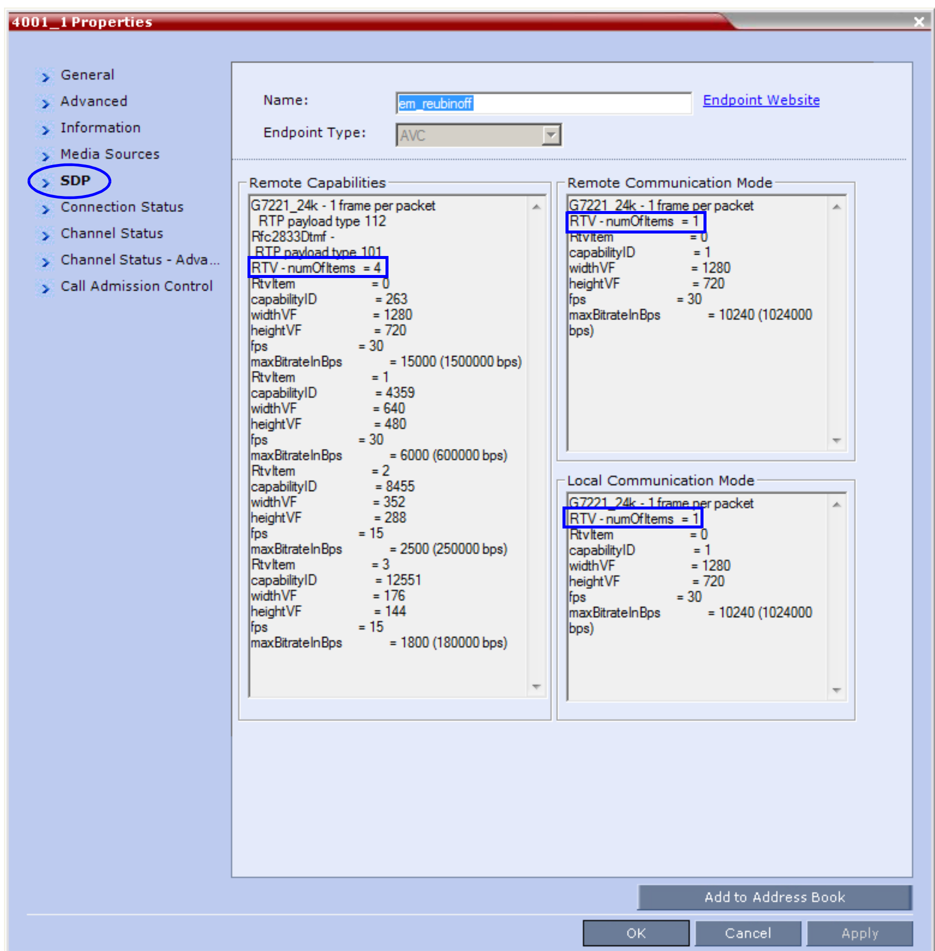
Lync Participants (RTV)

1 In the *Participant List* pane double-click the participant entry. Alternatively, right-click a participant and then click **Participant Properties**.

The *Participant Properties - General* dialog box opens.

2 Click the **SDP** tab.

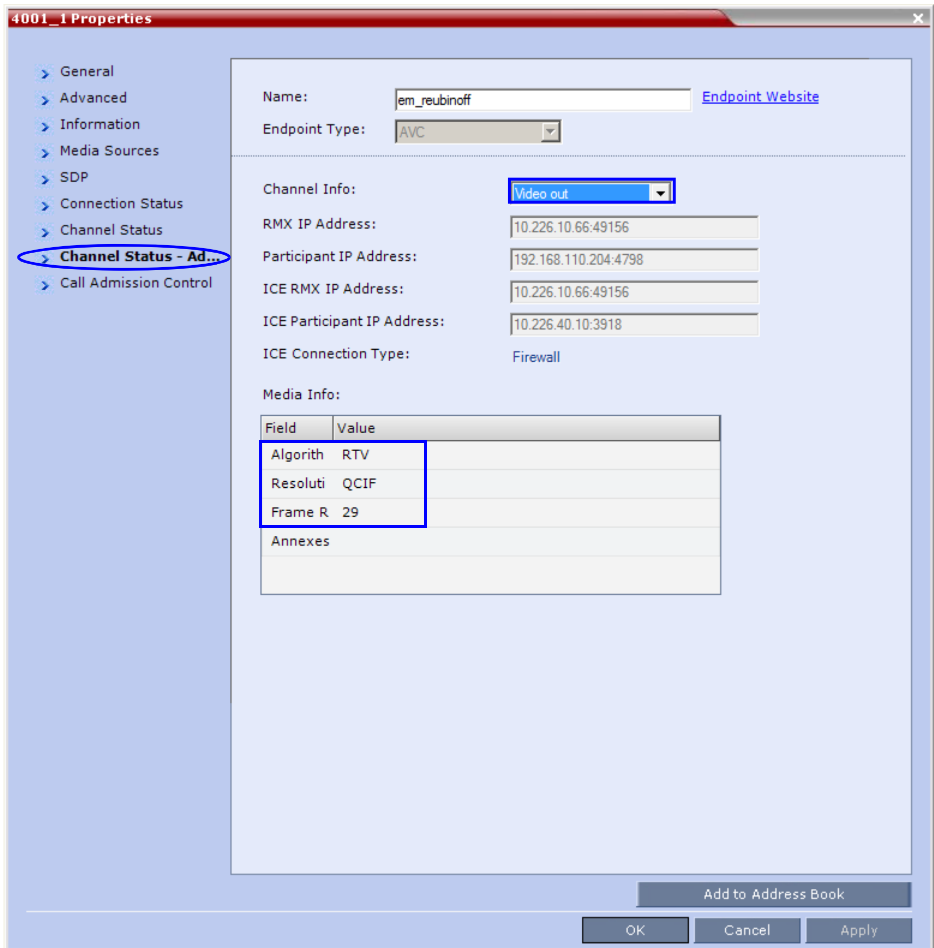
RTV is indicated in the *Remote Capabilities*, *Remote Communication Mode* and *Local Communication Mode* panes:



3 Click the **Channel Status - Advanced** tab

4 In the *Channel Info* drop-down menu select **Video Out.**

Media Info displays *RTV Channel Status* parameters:



Known Limitations

The following may occur in the collaborative environment:

- Artifacts and ghosting may appear when *Lync Clients* and *CTS* endpoints connect to the *VMR*.
  Frequency: Seldom.
- *Lync Client* receives fast updates (*Intra*) from *CTS 500* endpoints causing the screen to refresh repeatedly.
  Frequency: Often.
- Audio volume and video quality decreases on *CTS* endpoints.
  Frequency: Seldom.
- *CTS* endpoint connects and then disconnects after a few seconds.
  Frequency: Seldom.
- *Lync Clients* always connect *encrypted* to *non-encrypted* conferences.
- *Auto Layout* sometimes ignored for *CTS* and *Lync Clients* calling through *DMA*.
  Frequency: Rarely.
- *Content* sent from *HDX* endpoint is received by all endpoints for 1 second before stopping. Conference is *Content to Legacy* enabled and *TIP Compatibility* is *Video Only*.
  Frequency: Often.

Appendix J

Restoring Defaults

USB Restore Defaults

The *USB* port of an MCU in *Ultra Secure Mode* can be used to:

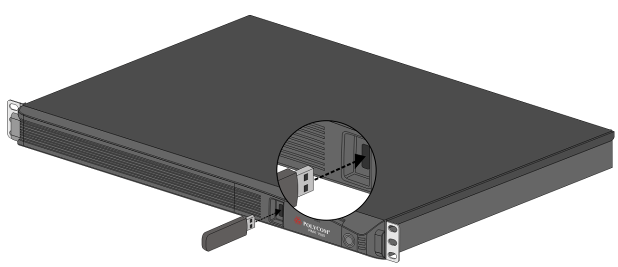
- Restore the MCU to *Factory Security Defaults* mode *(https → http)*.
- Perform a *Comprehensive Restore to Factory Defaults*
- Perform an *Emergency CRL (Certificate Revocation List) Update*

USB Ports on RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000

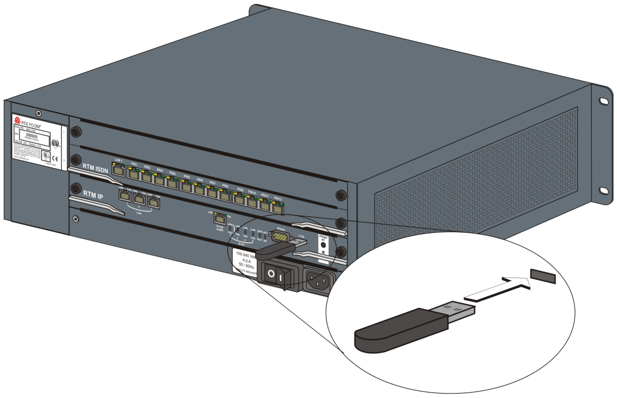
Do **not** use any *USB* ports other than the ones indicated in the following diagrams.

When performing *USB Operations*, the following *USB* ports are used:

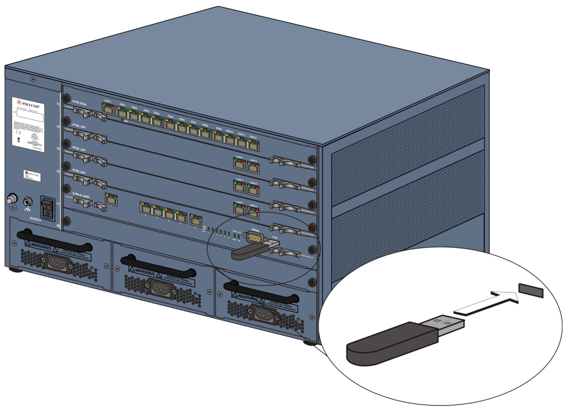
- RealPresence Collaboration Server (RMX) 1500 - left most *USB* port on the **front panel**.



- RealPresence Collaboration Server (RMX) 2000 - at the bottom right corner of the *RTM IP* card on the **back panel**.



- RealPresence Collaboration Server (RMX) 4000 - at the bottom right corner of the *RTM IP 4000* card on the **back panel.**



Restore to Factory Security Defaults

Restore to Factory Security Defaults can be performed by either:

- Inserting a *USB* device such as a mouse or a keyboard into the MCU's *USB Port* causing it to exit *Ultra Secure Mode* and return to *Factory Security Defaults* mode. After performing this procedure, logins to the MCU use the **http** command and not the **https** command.

  or

- Inserting a *USB* key containing a file named *RestoreFactorySecurityDefaults.txt*.

To restore the MCU to Factory Security Defaults:

1 Insert a USB device or a *USB* key containing a file named *RestoreFactorySecurityDefaults.txt* into the *USB* port of the MCU.

The *USB* port locations for *RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 2000/*RealPresence Collaboration Server (RMX) 4000 are shown in "*USB Ports on RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000"* on page **J-1**.

2 Power the MCU **Off** and then **On**.

3 Login using **http**://<Control Unit IP Address>.

Comprehensive Restore to Factory Defaults

Inserting a *USB* key containing a file named *RestoreToFactoryDefault.txt* **and** a l*an.cfg* file will cause the MCU to exit *Secure Mode* **and** perform a *Comprehensive Restore to Factory Defaults*.

The *Comprehensive Restore to Factory Defaults* deletes the following files:

- CDR
- Address Book
- Log Files
- Faults
- Dump Files
- Notes

In addition all the conferencing entities are deleted:

- Entry Queues
- Profiles
- Meeting Rooms
- IVR Services
- Default Network IP Service
- Log Files
- CFS license information
- Management Network Service

The MCU is restored to the settings it had when shipped from the factory. The *Product Activation Key* is required to re-configure the *Management Network Service* during the *First Entry Configuration.*

Comprehensive Restore to Factory Defaults Procedure

To perform a Comprehensive Restore to Factory Defaults:

Restoring the *MCU* to *Factory Defaults* consists of the following procedures:

A Backup Configuration Files

— These files will be used to restore the system in Procedure **C**.

B Restore to Factory Defaults

— Restart the system with a *USB* device containing a file named *RestoreToFactoryDefault.txt* and a *lan.cfg* file plugged into the *USB* port.

C Optional. Restore the System Configuration From the Backup

— Apply the backup file created in procedure **A**.

— Restart the MCU.

(If the MCU is unresponsive after these procedures a further restart may be necessary.)

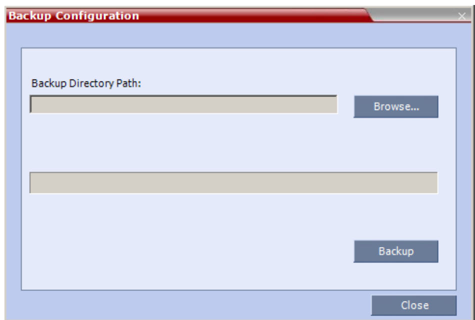
Procedure A: Backup Configuration Files

The *Software Management* menu is used to backup and restore the MCU's configuration files and to download MCU software.

To backup configuration files:

1 On the *RMX Menu*, click **Administration > Software Management > Backup Configuration**.

The *Backup Configuration* dialog box opens.



2 **Browse** to the *Backup Directory Path* and then click **Backup**.

Procedure B: Restore to Factory Defaults

To perform a Comprehensive Restore to Factory Default perform the following steps:

1 Insert a *USB* device containing a file named *RestoreToFactoryDefault.txt* and a *lan.cfg* file into the *USB* port of the MCU.
For more information on creating a lan.cfg file see the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide*, "*Modifying the Factory Default Management Network Settings on the USB Key*” on page **2-6**.

2 Power the MCU Off.

3 Power the MCU On.

4 Proceed from Step 2 of "*Procedure 1: First-time Power-up*” on page **2-19**, continuing to the end of Chapter 2 of the *RealPresence Collaboration Server (RMX) 1500/2000/4000 Getting Started Guide*.

5 Optional. Restore the system using *Procedure C: Restore the System Configuration From the Backup* below.

Procedure C: Restore the System Configuration From the Backup

To restore configuration files:

1 On the *RMX Menu*, click **Administration > Software Management > Restore Configuration**.

2 Browse to the *Restore Directory Path* where the backed up configuration files are stored.

3 Click the **Restore** button.

4 When the **Restore** is complete, restart the MCU.

MCU system settings, with the exception of *User* data, are restored.

5 Restore *User* data by repeating **Step 1** to **Step 3** of this procedure.

Appendix K

SIP RFC Support

Table K-1 SIP RFC Support in RealPresence Collaboration Server (RMX) Systems

SIP RFC	Description	Note
1321	MD5	
2032	RTP Payload for H.261	
2205	RSVP	
2327	Session Description Protocol (SDP)	
2429	RTP Payload for H.263+	
2833	RTP Payload for DTMF	
2617	HTTP Authentication	
2976	SIP Info Method	
3261	SIP	
3264	Offer/Answer Model	
3265	SIP Specific Event Notification	Limited support
3266	SDP Support for IPv6	
3311	SIP Update Method	
3515	SIP Refer Method	Limited support
3550	RTP	
3551	RTP Profile for Audio/Video	
3711	SRTP	
3890	Transport Independent Bandwidth Modifier for SDP	
3891	SIP Replaces header	Limited support
3892	SIP Referred-by Mechanism	Limited support
3984	RTP Payload format for H.264	
4028	Session Timers in SIP	
4145	TCP Media Transport in SDP	

Table K-1 SIP RFC Support in RealPresence Collaboration Server (RMX) Systems (Continued)

SIP RFC	Description	Note
4566	Session Description Protocol(SDP)	
4568	SDP Security Descriptions	
4573	H.224 RTP Payload (FECC)	
4574	SDP Label Attribute	
4582	Binary Floor Control Protocol (BFCP)	
4583	SDP for BFCP	
4796	SDP Content Attribute	
5168	XML Schema for Media Control (Fast Update)	
cc-transfer	Call Transfer Capabilities in SIP	Limited support
draft-ice-19	ICE spec for firewall traversal in SIP	
draft-turn-07	TURN spec for firewall traversal in SIP	
draft-rfc3489bis-15	STUN spec for firewall traversal in SIP	

Appendix L

Homologation for Brazil

H.323 & SIP Protocol Flag Options

Using a set of system flags, the user has the ability to select either Polycom proprietary or H.323/SIP standard protocol settings.

H.323 & SIP Flag Settings

Three flags are enabled on the MCU, allowing the user to define and select either standard or proprietary H.323 and SIP protocol settings.

Flag name: SIP_TIMERS_SET_INDEX

Description: SIP Timer type timeout settings according to standard or proprietary protocol.

Flag section: CS_MODULE_PARAMETERS

Possible Values: either 0 or 1.

0 - Polycom standard (flag default setting)

1 - SIP Standard recommendation. For homologation and certification testing, this flag must be set to 1.

For use as a reference, Table 1 lists the SIP timer types for each flag setting and their corresponding timeout values in milliseconds.

Table 1 *SIP Timer Types & their Values*

SIP TIMER Types	Value (in milliseconds)	
	POLYCOM (flag default)	**Standard Recommended**
T1	50000	500
T2	20000	4000
TimerB	35000	32000
TimerC	35000	60000
TimerD	32000	32000
TimerF	35000	32000
TimerH	35000	32000
TimerI	5000	5000
TimerJ	32000	32000

Table 1 *SIP Timer Types & their Values (Continued)*

SIP TIMER Types	Value (in milliseconds)	
	POLYCOM (flag default)	**Standard Recommended**
TimerK	5000	5000

Flag name: H323_TIMERS_SET_INDEX

Flag description: Enables or disables H.323 index timer according to standard or proprietary H.323 protocol.

Section CS_MODULE_PARAMETERS

Possible values:

0 - Sets the H.323 index timer to Polycom proprietary (flag default setting)

1 - Sets the H.323 index timer based on the H.323 Standard recommendation. For homologation and certification testing, this flag must be set to 1.

Flag name: DISABLE_DUMMY_REGISTRATION

Flag description: Enables or disables SIP dummy registration on the domain.

Flag Section: MCMS_PARAMETERS_USER

Possible values:

NO - Disables SIP dummy registration (flag default setting).

YES - Enables SIP dummy registration. For homologation and certification testing, the flag must be set to YES.